Division polynomials and canonical local heights on hyperelliptic Jacobians

AUTHOR(S):

Uchida, Yukihiro

CITATION:

Uchida, Yukihiro. Division polynomials and canonical local heights on hyperelliptic Jacobians. manuscripta mathematica 2011, 134(3-4): 273-308

ISSUE DATE:

2011-03

URL:

http://hdl.handle.net/2433/134800

manuscripta mathematica manuscript No.
(will be inserted by the editor)

Yukihiro Uchida

Division polynomials and canonical local heights on hyperelliptic Jacobians

Received: date / Revised version: date

Abstract. We generalize the division polynomials of elliptic curves to hyperelliptic Jacobians over the complex numbers. We construct them by using the hyperelliptic sigma function. Using the division polynomial, we describe a condition that a point on the Jacobian is a torsion point. We prove several properties of the division polynomials such as a determinantal expression and recurrence formulas. We also study relations among the sigma function, the division polynomials, and the canonical local height functions.

1. Introduction

In the study of elliptic curves, the division polynomials are important for the study of the structure of the torsion subgroup. Moreover the division polynomials have various applications such as description of a multiplication map, computation of the order of the Mordell-Weil group of an elliptic curve over a finite field, elliptic divisibility sequences, and transformation formulas for canonical local heights.

Recently, several authors studied generalizations of the division polynomials. They defined the division polynomials in the cases of hyperelliptic curves and hyperelliptic Jacobians.

The former case is studied by D. G. Cantor [9] and Ônishi [24–26]. Cantor algebraically defined an analog of the division polynomial on a hyperelliptic curve of any genus over any field. On the other hand, Ônishi studied the hyperelliptic sigma function, which is a generalization of the Weierstrass sigma function. Then he defined an analog of the division polynomial on a hyperelliptic curve of any genus over $\mathbb{C}$ by using the hyperelliptic sigma function and its derivatives. He also proved a determinantal expression of it. Matsutani [26, Appendix] proved that these two analogs of the division polynomial are essentially the same.

The latter case is studied by Kanayama [15,16] in the case of genus 2. He defined the division polynomials on the Jacobian variety of a curve of genus 2, and described the multiplication maps by using them and their derivatives. He also described a condition that a point on the Jacobian is a torsion point by using the division polynomial and its derivatives.

Yukihiro Uchida: Department of Mathematics, Faculty of Science, Kyoto University, Kyoto 606-8502, Japan. e-mail: uchida@math.kyoto-u.ac.jp

Mathematics Subject Classification (2000): Primary 14H40, Secondary 11G10, 11G50

In this paper, we generalize Kanayama's division polynomials to the case of general hyperelliptic Jacobians. The hyperelliptic sigma function is defined for any genus, thus we can define the division polynomials in the same way as in the case of elliptic curves.

To state our results, we make some definitions. Let C be a non-singular projective hyperelliptic curve of genus g over $\mathbb{C}$ defined by

$$y^2 = x^{2g+1} + \lambda_{2g}x^{2g} + \cdots + \lambda_1 x + \lambda_0.$$

Let $J = \mathbb{C}^g/\Lambda$ be the Jacobian variety of C. Let $\sigma\colon \mathbb{C}^g \to \mathbb{C}$ be the hyperelliptic sigma function. We denote by Θ the theta divisor of J defined by $\sigma(u) = 0$.

We define the division polynomial $\phi_n(u)$ by

$$\phi_n(u) = \frac{\sigma(nu)}{\sigma(u)^{n^2}}$$

for any integer n.

Similarly to the case of genus 1, the hyperelliptic $\wp$-functions are defined as follows:

$$\wp_{ij}(u) = -\frac{\partial^2}{\partial u_i \partial u_j}\log\sigma(u),$$
$$\wp_{ijk}(u) = -\frac{\partial^3}{\partial u_i \partial u_j \partial u_k}\log\sigma(u)$$

for $1 \le i, j, k \le g$. Then ϕ_n, $\wp_{ij}$, and $\wp_{ijk}$ are periodic with respect to Λ. For $P = u \bmod \Lambda \in J$, we write $\phi_n(P) = \phi_n(u)$, $\wp_{ij}(P) = \wp_{ij}(u)$ and $\wp_{ijk}(P) = \wp_{ijk}(u)$.

In the case of elliptic curves, it is known that the division polynomial ϕ_n is represented as a polynomial in the Weierstrass $\wp$-function and its derivative. More precisely, if $\wp(u)$ satisfy the differential equation

$$\wp'(u)^2 = 4\wp(u)^3 + 4\lambda_1\wp(u) + 4\lambda_0,$$

then ϕ_n is represented as a polynomial in $\wp$ and $\wp'$ with coefficients in $\mathbb{Z}[\lambda_0, \lambda_1]$.

For any genus, we can prove the following:

Theorem 1.1 (cf. Theorem 5.8). *There exists a non-zero computable element $\Delta \in \mathbb{Z}[\lambda_0, \ldots, \lambda_{2g}]$ such that, for any integer n, ϕ_n is represented as a polynomial in $\wp_{ij}$ and $\wp_{ijk}$ $(1 \le i, j, k \le g)$ with coefficients in $\mathbb{Z}[1/\Delta, \lambda_0, \ldots, \lambda_{2g}]$.*

Theorem 1.1 is proved by a determinantal expression of ϕ_n (cf. Theorem 5.7) and the theory of Gröbner bases in a polynomial ring over a general Noetherian ring. In particular, we can take $\Delta = 2$ for $g = 2$. See Example 5.9.

Kanayama [15] gave the multiplication formulas for the $\wp$-functions by using the division polynomial ϕ_n. We can give the same multiplication formulas as his formulas for any genus (Proposition 4.10). Kanayama also gave a condition that a point in the Jacobian is a torsion point. Using the vanishing structure of the sigma function and its derivatives proved by Ônishi [26], we can prove a generalization of Kanayama's result.

Theorem 1.2 (cf. Theorem 4.7). *Let n be a non-zero integer and $P \in J \setminus \Theta$. Then $[n]P = O$ if and only if $(\phi_n)_{\natural^m}(P) = 0$ for all $m = 1, 2, \ldots, g$, where $(\phi_n)_{\natural^m}$ is the derivative of ϕ_n defined at the end of Section 2.*

In fact, in the case of genus 2, Theorem 1.2 is a refinement of Kanayama's theorem. See Remark 4.8.

In the case of elliptic curves, the division polynomial has a determinantal expression. Let n be a positive integer. Then we have

$$\phi_n(u) = \frac{(-1)^{n-1}}{(1!2!\cdots(n-1)!)^2} \begin{vmatrix} \wp'(u) & \wp''(u) & \cdots & \wp^{(n-1)}(u) \\ \wp''(u) & \wp'''(u) & \cdots & \wp^{(n)}(u) \\ \vdots & \vdots & \ddots & \vdots \\ \wp^{(n-1)}(u) & \wp^{(n)}(u) & \cdots & \wp^{(2n-3)}(u) \end{vmatrix}.$$

This formula is called the Kiepert formula. We can deduce this formula from the Frobenius-Stickelberger formula, which is a kind of addition formula for the sigma function. Ônishi [24–26] generalized the Frobenius-Stickelberger formula to general hyperelliptic Jacobians. By using his formula, we can prove the Kiepert-type formula, which is a determinantal expression of the division polynomial. It is too complicated to include here, see Theorem 5.5. Moreover, we give another determinantal expression (Theorem 5.7), which is used in the proof of Theorem 1.1.

The division polynomials of an elliptic curve satisfy a recurrence formula as follows: For integers m and n,

$$\phi_{m+n}(u)\phi_{m-n}(u) = \phi_n(u)^2\phi_{m+1}(u)\phi_{m-1}(u) - \phi_m(u)^2\phi_{n+1}(u)\phi_{n-1}(u). \tag{1}$$

This formula is important for the computation of the division polynomials and the study of elliptic divisibility sequences.

Recently, Kanayama [16] proved a generalization of (1) which includes some derivatives of the division polynomials. By using a classical theta relation, we have the following generalization of (1), which is different from Kanayama's formula.

Theorem 1.3 (cf. Theorem 6.4). *Let $n > 2^g$ be an integer, $m_1, m_2, \ldots, m_n$ be integers and $u \in \mathbb{C}^g$. We define the $n \times n$ matrix A by*

$$A = \left(\phi_{m_i+m_j}(u)\phi_{m_i-m_j}(u)\right)_{1\le i,j\le n}.$$

Then we have $\det A = 0$. In particular, if $g \equiv 1, 2 \pmod 4$ and n is even, then we have $\mathrm{pf}\, A = 0$, where $\mathrm{pf}\, A$ is the Pfaffian of A.

In fact, we can deduce (1) from Theorem 1.3 when $g = 1$.

As an application of the division polynomials, we study relations among the sigma function, the division polynomials, and the canonical local height functions. We first prove an explicit formula for the canonical local height functions for Archimedean places. Then we prove transformation formulas for the canonical local height functions for any places. More precisely, we prove the following results.

We assume that C is defined over a number field K. Then we may regard J as an algebraic variety defined over K. Moreover the theta divisor Θ is defined over

K. By Theorem 1.1, ϕ_n may be regarded as a rational function on J defined over K.

Let v be a place of K and K_v be the completion of K at v. Then the canonical local height function $\hat{\lambda}_v$ is an $\mathbb{R}$-valued function defined on $(J \setminus \Theta)(K_v)$ (see Definition 7.2).

First let v be an Archimedean place. We may regard $(J \setminus \Theta)(K_v)$ as a subset of $(J \setminus \Theta)(\mathbb{C})$ via an embedding $K_v \hookrightarrow \mathbb{C}$. By using the hyperelliptic sigma function, we have an explicit formula for the canonical local height function $\hat{\lambda}_v$ as follows:

Theorem 1.4 (cf. Theorem 7.4). *Let v be an Archimedean place. For any $P \in (J \setminus \Theta)(K_v)$,*

$$\hat{\lambda}_v(P) = -\log \left| \exp\left(-\pi\sqrt{-1}L(u,u)\right) \sigma(u) \right|,$$

where $u \in \mathbb{C}^g$ is a point with $P = u \bmod \Lambda$ and $L(z,w)$ is the $\mathbb{R}$-bilinear form on $\mathbb{C}^g \times \mathbb{C}^g$ defined in Section 2.

When $g = 1$, this formula is well-known (cf. [28, Chapter VI, Theorem 3.2]). When $g = 2$, it was proved by Yoshitomi [32, Corollary 2.5].

Next we assume that v is any place of K. We can prove the transformation formula, which relates a multiplication map, the canonical local height function and the division polynomial.

Theorem 1.5 (cf. Theorem 7.5). *Let v be a place of K. Let n be a non-zero integer and $P \in J(K_v)$. If $P, [n]P \notin \Theta$, then we have*

$$\hat{\lambda}_v([n]P) = n^2 \hat{\lambda}_v(P) - \log |\phi_n(P)|_v,$$

where $|\cdot|_v$ is an absolute value associated with v.

Note that Theorem 1.5 for Archimedean places is an immediate consequence of Theorem 1.4. Theorem 1.5 is also known in the case of genus 1 (cf. [28, Chapter VI, Exercise 4 (e)]).

This paper is organized as follows. In Section 2, we review the theory of hyperelliptic functions. In Section 3, we study division of hyperelliptic functions, which is used in computation of the division polynomials. We use the theory of Gröbner bases in a polynomial ring over a general Noetherian ring to prove lemmas in this section. In Section 4, we define the division polynomials and prove some properties of them. In Section 5, we derive determinantal formulas, which express the division polynomial as a quotient of determinants. We also prove a theorem on the coefficients of the division polynomials. In Section 6, we first describe a classical relation of theta functions with characteristics. Then we prove recurrence formulas for the division polynomials by this relation. In Section 7, we give a definition and an explicit formula for the canonical local height function for an Archimedean place. Then we prove some relations of the canonical local height function and the addition or multiplication map.

Some examples require computation with computer algebra systems. The author used Macaulay 2 [13], Maxima [19], and Risa/Asir [23].

Notation

We use the following notation throughout the paper. For a matrix A, we denote by ${}^{\mathrm{t}}A$ the transpose of A. Unless otherwise stated, we regard a vector as a column vector and we write $u = {}^{\mathrm{t}}(u_1, u_2, \dots, u_g)$ for $u \in \mathbb{C}^g$. For a ring R, we denote by $M_n(R)$ the set of $n \times n$ matrices over R. We denote by 1_n the identity matrix of size n. For a $2n \times 2n$ skew-symmetric matrix A, we denote the Pfaffian of A by $\mathrm{pf}\, A$, that is, $\mathrm{pf}\, A = \sqrt{\det A}$. We take the sign of the Pfaffian so that

$$\mathrm{pf} \begin{pmatrix} 0 & -1_n \\ 1_n & 0 \end{pmatrix} = (-1)^{n+1}.$$

The choice only affects the addition formula (Theorem 2.15).

For a ring R and elements $r_1, \dots, r_m \in R$, we denote by $\langle r_1, \dots, r_m \rangle$ the ideal generated by $r_1, \dots, r_m$ in R.

For $z \in \mathbb{C}$, we define $\boldsymbol{e}(z) = \exp(2\pi\sqrt{-1}z)$. We denote by $\mathfrak{H}_g$ by the Siegel upper half space of degree g, that is,

$$\mathfrak{H}_g = \{\tau \in M_g(\mathbb{C}) \mid {}^{\mathrm{t}}\tau = \tau,\ \mathrm{Im}\,\tau \text{ is positive definite}\}.$$

In an expression for the Taylor expansion, the symbol $(d^\circ(z_1, z_2, \dots, z_m) \geq n)$ stands for the terms of total degree at least n with respect to the variables $z_1, z_2, \dots, z_m$. These terms may contain other variables.

2. The sigma function

In this section, we review the theory of the sigma function and fix the definitions. For details, we refer the reader to [5, 26]. Note that our choice of a defining equation of a curve and differential forms is the same as that in [26] but different from that in [5]. Hence our formulas are also different from those in [5].

Let C be a non-singular projective curve over $\mathbb{C}$ defined by

$$y^2 = f(x) = x^{2g+1} + \lambda_{2g}x^{2g} + \cdots + \lambda_1 x + \lambda_0.$$

Then $f(x)$ has no multiple roots, the genus of C is g, and C has the unique point ∞ at infinity. We define $\lambda_{2g+1} = 1$ for convention. To simplify notation, for a subring R of $\mathbb{C}$, we write $R[\lambda_i]$ instead of $R[\lambda_0, \lambda_1, \dots, \lambda_{2g}]$.

The differential forms

$$\omega_1 = \frac{dx}{2y}, \quad \omega_2 = \frac{xdx}{2y}, \quad \dots, \quad \omega_g = \frac{x^{g-1}dx}{2y}$$

form a basis of the holomorphic 1-forms on C. For $j = 1, 2, \dots, g$, we define

$$\eta_j = \frac{1}{2y} \sum_{k=j}^{2g-j} (k+1-j)\lambda_{k+1+j} x^k dx,$$

which is a differential form of the second kind without poles except at ∞. Let $\alpha_1, \dots, \alpha_g, \beta_1, \dots, \beta_g$ be a symplectic basis of $H_1(C, \mathbb{Z})$. Then their intersections

satisfy $\alpha_i \cdot \alpha_j = \beta_i \cdot \beta_j = 0$ and $\alpha_i \cdot \beta_j = \delta_{ij}$, where δ_{ij} is Kronecker's delta. We define the period matrices $\omega', \omega'', \eta', \eta'' \in M_g(\mathbb{C})$ by

$$\omega' = \left(\int_{\alpha_j} \omega_i \right), \quad \omega'' = \left(\int_{\beta_j} \omega_i \right),$$
$$\eta' = \left(-\int_{\alpha_j} \eta_i \right), \quad \eta'' = \left(-\int_{\beta_j} \eta_i \right).$$

Note that our definition differs from that in [26] by the signs of η' and η''. When $g = 2$, it coincides with the definition in [12, 15].

Let

$$M = \begin{pmatrix} \omega' & \omega'' \\ \eta' & \eta'' \end{pmatrix}.$$

Then we have the generalized Legendre relation (cf. [5, Lemma 2.0.1]):

$$M \begin{pmatrix} 0 & -1_g \\ 1_g & 0 \end{pmatrix} {}^{\mathrm{t}}M = -2\pi\sqrt{-1} \begin{pmatrix} 0 & -1_g \\ 1_g & 0 \end{pmatrix}. \tag{2}$$

In particular, $\tau = \omega'^{-1}\omega''$ is a symmetric matrix, and we have

$$\eta'' = \eta'\tau - 2\pi\sqrt{-1}\,{}^{\mathrm{t}}\omega'^{-1}.$$

By Riemann's inequality, $\mathrm{Im}\,\tau$ is positive definite, hence $\tau \in \mathfrak{H}_g$.

We define the theta function with characteristics by

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z, \tau) = \sum_{n \in \mathbb{Z}^g} \boldsymbol{e} \left(\frac{1}{2} {}^{\mathrm{t}}(n+a)\tau(n+a) + {}^{\mathrm{t}}(n+a)(z+b) \right),$$

where $z \in \mathbb{C}^g$, $\tau \in \mathfrak{H}_g$ and $a, b \in \mathbb{R}^g$.

Let $\Lambda = \omega'\mathbb{Z}^g + \omega''\mathbb{Z}^g$. Then Λ is a lattice of $\mathbb{C}^g$. Let

$$\delta'' = {}^{\mathrm{t}}\left(\frac{1}{2}, \ldots, \frac{1}{2} \right), \quad \delta' = {}^{\mathrm{t}}\left(\frac{g}{2}, \frac{g-1}{2}, \ldots, \frac{1}{2} \right), \quad \delta = \begin{pmatrix} \delta'' \\ \delta' \end{pmatrix}.$$

We define the hyperelliptic sigma function on $\mathbb{C}^g$ by

$$\sigma(u) = c \exp\left(\frac{1}{2} {}^{\mathrm{t}}u\eta'\omega'^{-1}u \right) \vartheta[\delta](\omega'^{-1}u, \tau),$$

where c is the constant such that $\sigma(u)$ satisfies the following proposition:

Proposition 2.1. *The sigma function $\sigma(u)$ has the Taylor expansion around $u = 0$ with coefficients in $\mathbb{Q}[\lambda_i]$. Furthermore, if $g = 2l - 1$ or $g = 2l$, then we have*

$$\sigma(u) = \begin{vmatrix} u_1 & u_2 & \ldots & u_l \\ u_2 & u_3 & \ldots & u_{l+1} \\ \vdots & \vdots & \ddots & \vdots \\ u_l & u_{l+1} & \ldots & u_{2l-1} \end{vmatrix} + (d^\circ(u_1, u_2, \ldots, u_g) \geq l+2).$$

Proof. The former part is proved more generally in [7, Corollary 1] or in [22, Theorem 3]. The latter part is proved in [5, Proposition 2.2]. □

We can also determine the constant c explicitly, see [5, Definition 2.1]. We will not use an explicit expression of the constant c later. Note that our definition of the sigma function coincides with that in [26].

For any $u \in \mathbb{C}^g$, we denote by u' and u'' the elements in $\mathbb{R}^g$ satisfying that $u = \omega' u' + \omega'' u''$. We define the $\mathbb{C}$-valued $\mathbb{R}$-bilinear form $L(u, v)$ on $\mathbb{C}^g \times \mathbb{C}^g$ by

$$L(u,v) = \frac{1}{2\pi\sqrt{-1}} {}^{\mathrm{t}}u(\eta' v' + \eta'' v'').$$

For $l \in \Lambda$, let

$$\chi(l) = \boldsymbol{e}\left(\left({}^{\mathrm{t}}l'\delta'' - {}^{\mathrm{t}}l''\delta'\right) + \frac{1}{2}{}^{\mathrm{t}}l'l''\right).$$

Note that $\chi(l) = \pm 1$.

Proposition 2.2 (Translational relation). *For any $u \in \mathbb{C}^g$ and any $l \in \Lambda$, we have*

$$\sigma(u+l) = \chi(l)\boldsymbol{e}\left(L\left(u + \frac{1}{2}l, l\right)\right)\sigma(u).$$

Proof. This proposition is proved by using formulas for theta functions and the generalized Legendre relation. See [5, Theorem 1.1]. □

Proposition 2.3. *The sigma function $\sigma(u)$ is an odd function if $g \equiv 1, 2 \pmod 4$, and an even function if $g \equiv 0, 3 \pmod 4$.*

Proof. It follows from [20, Chapter II, Proposition 3.14]. □

Let

$$E(u,v) = L(u,v) - L(v,u).$$

Then $E(u, v)$ is the imaginary part of the Riemann form associated with $\sigma(u)$. Moreover we have the following proposition.

Proposition 2.4. *We have the following properties.*

(i) $E(u, v)$ *is $\mathbb{R}$-valued, $\mathbb{R}$-bilinear and alternating.*
(ii) $E(\sqrt{-1}u, \sqrt{-1}v) = E(u, v)$.
(iii) $E(u, v)$ *is $\mathbb{Z}$-valued on $\Lambda \times \Lambda$.*
(iv) $E(u,v) = {}^{\mathrm{t}}u''v' - {}^{\mathrm{t}}u'v''$.

Proof. (i) and (iii) follow from (iv). (ii) follows from [17, Chapter VI, Theorem 1.2]. We prove (iv).

$$\begin{aligned}
E(u,v) &= L(u,v) - L(v,u) \\
&= \frac{1}{2\pi\sqrt{-1}}\Big({}^{\mathrm{t}}(\omega' u' + \omega'' u'')(\eta' v' + \eta'' v'') \\
&\quad - {}^{\mathrm{t}}(\omega' v' + \omega'' v'')(\eta' u' + \eta'' u'')\Big) \\
&= \frac{1}{2\pi\sqrt{-1}}\left({}^{\mathrm{t}}u'({}^{\mathrm{t}}\omega'\eta'' - {}^{\mathrm{t}}\eta'\omega'')v'' + {}^{\mathrm{t}}u''({}^{\mathrm{t}}\omega''\eta' - {}^{\mathrm{t}}\eta''\omega')v'\right).
\end{aligned}$$

By the generalized Legendre relation (2), we have

$$ {}^{\mathrm{t}}\eta'\omega'' - {}^{\mathrm{t}}\omega'\eta'' = {}^{\mathrm{t}}\omega''\eta' - {}^{\mathrm{t}}\eta''\omega' = 2\pi\sqrt{-1}\,1_g. $$

Hence we have $E(u,v) = {}^{\mathrm{t}}u''v' - {}^{\mathrm{t}}u'v''$. □

We define the hyperelliptic $\wp$-functions by

$$ \wp_{ij}(u) = -\frac{\partial^2}{\partial u_i \partial u_j}\log\sigma(u), $$
$$ \wp_{ijk}(u) = -\frac{\partial^3}{\partial u_i \partial u_j \partial u_k}\log\sigma(u),\ \ldots, \quad i,j,k,\ldots \in \{1,2,\ldots,g\}. $$

Obviously, $\wp$-functions do not depend on the order of their indices. For example, $\wp_{ij}(u) = \wp_{ji}(u)$.

Proposition 2.5. *For any $u \in \mathbb{C}^g$ and any $l \in \Lambda$, we have*

$$ \wp_{ij}(u+l) = \wp_{ij}(u),\ \wp_{ijk}(u+l) = \wp_{ijk}(u),\ \ldots, $$

that is, the hyperelliptic $\wp$-functions are periodic with respect to Λ.

Proof. Take the logarithmic derivatives of both sides of the translational relation (Proposition 2.2). □

Let $J = \mathbb{C}^g/\Lambda$ be the Jacobian variety of C and $\kappa\colon \mathbb{C}^g \to J$ be the natural projection. By Proposition 2.5, we may regard $\wp_{ij}$, $\wp_{ijk}$, … as meromorphic functions on J. We write $\wp_{ij}(P) = \wp_{ij}(u)$ for $P = \kappa(u)$.

We define the Abel-Jacobi map $I\colon \mathrm{Pic}^0(C) \to J$ by

$$ I\left(\sum_{i=1}^m n_i P_i\right) = \kappa\left({}^{\mathrm{t}}\left(\sum_{i=1}^m n_i \int_\infty^{P_i} \omega_1, \ldots, \sum_{i=1}^m n_i \int_\infty^{P_i} \omega_g\right)\right), $$

where $\sum_{i=1}^m n_i = 0$. By the Abel-Jacobi theorem, the map I is well-defined and a group isomorphism.

The following theorem gives the inverse of the Abel-Jacobi map.

Theorem 2.6. *Let $(x_1,y_1),(x_2,y_2),\ldots,(x_g,y_g) \in C$ and*

$$ u = {}^{\mathrm{t}}\left(\sum_{i=1}^g \int_\infty^{(x_i,y_i)} \omega_1, \ldots, \sum_{i=1}^g \int_\infty^{(x_i,y_i)} \omega_g\right), $$

that is, $\kappa(u) = I(\sum_{i=1}^g (x_i,y_i) - g\infty)$. Then we have

$$ 2y_i = \wp_{ggg}(u)x_i^{g-1} + \wp_{gg,g-1}(u)x_i^{g-2} + \cdots + \wp_{gg2}(u)x_i + \wp_{gg1}(u), $$
$$ x_i^g = \wp_{gg}(u)x_i^{g-1} + \wp_{g,g-1}(u)x_i^{g-2} + \cdots + \wp_{g2}(u)x_i + \wp_{g1}(u). $$

In particular,

$$ \wp_{gi}(u) = (-1)^{g-i}e_{g-i+1}, $$

where e_i is the i-th elementary symmetric polynomial in $x_1, x_2, \ldots, x_g$.

Proof. See [5, Theorem 3.2]. □

For an integer n with $1 \leq n \leq g$, let

$$\Theta^{[n]} = \left\{ I\left(\sum_{i=1}^{n} P_i - n\infty\right) \;\middle|\; P_1, \ldots, P_n \in C \right\}.$$

We define $\Theta^{[0]} = \{O\}$. Then, for $0 \leq n \leq g$, $\Theta^{[n]}$ is a closed subvariety of J and $\dim \Theta^{[n]} = \min\{n, g\}$. Furthermore $\Theta^{[g]} = J$. We define the theta divisor Θ by $\Theta = \Theta^{[g-1]}$.

Proposition 2.7. *The divisor of $\sigma(u)$ is $\kappa^{-1}(\Theta)$.*

Proof. See [21, pp. 3.80–82]. Note that this proposition is a special case of Theorem 2.17 (ii). □

By Proposition 2.7, $\wp_{i_1 i_2 \ldots i_n}$ has a pole of order n along Θ. We can prove the converse. To state it, we introduce the following notation. Let R be a subring of $\mathbb{C}$. We write

$$\begin{aligned} R[\wp_{gi}, \wp_{ggi}] &= R[\wp_{g1}, \wp_{g2}, \ldots, \wp_{gg}, \wp_{gg1}, \wp_{gg2}, \ldots, \wp_{ggg}], \\ R[\wp_{ij}] &= R[\{\wp_{ij} \mid 1 \leq i \leq j \leq g\}], \\ R[\wp_{ij}, \wp_{ijk}] &= R[\{\wp_{ij} \mid 1 \leq i \leq j \leq g\} \cup \{\wp_{ijk} \mid 1 \leq i \leq j \leq k \leq g\}]. \end{aligned}$$

For indeterminates X_{ij} and X_{ijk}, we similarly define $R[X_{gj}, X_{ggi}]$, $R[X_{ij}]$ and $R[X_{ij}, X_{ijk}]$. When we consider these rings, we ignore the order of the indices of the indeterminates. For example, we identify X_{ig} as X_{gi}.

Theorem 2.8. *Let $\varphi\colon J \setminus \Theta \to \mathbb{C}^{2g}$ be the morphism defined by*

$$\varphi(P) = (\wp_{g1}(P), \wp_{g2}(P), \ldots, \wp_{gg}(P), \wp_{gg1}(P), \wp_{gg2}(P), \ldots, \wp_{ggg}(P)).$$

Then φ is an embedding, therefore the affine ring of $J \setminus \Theta$ is isomorphic to $\mathbb{C}[\wp_{gi}, \wp_{ggi}]$. In particular, any meromorphic function on J which has a pole only along Θ is represented as a polynomial in $\wp_{g1}$, $\wp_{g2}$, …, $\wp_{gg}$, $\wp_{gg1}$, $\wp_{gg2}$, …, $\wp_{ggg}$.

Theorem 2.8 is proved by using Mumford's construction of hyperelliptic Jacobians [21]. Furthermore, we can determine the structure of the ring $\mathbb{C}[\wp_{gi}, \wp_{ggi}]$. We introduce some polynomials to describe it, following [21, Chapter IIIa, §1]. Let

$$\begin{aligned} U(t) &= t^g + U_1 t^{g-1} + \cdots + U_g, \\ V(t) &= \quad V_1 t^{g-1} + \cdots + V_g. \end{aligned}$$

By the division algorithm, we have

$$f(t) - V(t)^2 = U(t)W(t) + R_1 t^{g-1} + \cdots + R_{g-1} t + R_g,$$

where $W(t)$ is a polynomial in t, and $R_1, R_2, \dots, R_g$ are polynomials in U_1, U_2, $\dots$, U_g, V_1, V_2, $\dots$, V_g with coefficients in $\mathbb{Z}[\lambda_i]$.

To adopt them to our coordinates $\wp_{gi}$ and $\wp_{ggi}$, we define the polynomials F_1, F_2, $\dots$, F_g in $X_{g1}, X_{g2}, \dots, X_{gg}, X_{gg1}, X_{gg2}, \dots, X_{ggg}$ by

$$\begin{aligned} &F_i(X_{g1}, X_{g2}, \dots, X_{gg}, X_{gg1}, X_{gg2}, \dots, X_{ggg}) \\ &\quad = 4R_i\left(-X_{gg}, -X_{g,g-1}, \dots, -X_{g1}, \frac{1}{2}X_{ggg}, \frac{1}{2}X_{gg,g-1}, \dots, \frac{1}{2}X_{gg1}\right), \end{aligned}$$

where we substitute $-X_{gj}$ and $X_{ggj}/2$ for U_{g-j+1} and V_{g-j+1} respectively in the right-hand side. We can easily verify that $F_1, F_2, \dots, F_g \in \mathbb{Z}[\lambda_i][X_{gi}, X_{ggi}]$. Then we can determine the structure of the affine ring of $J \setminus \Theta$ as follows:

Theorem 2.9. *The homomorphism*

$$\begin{aligned} \mathbb{C}[X_{gi}, X_{ggi}]/\langle F_1, F_2, \dots, F_g\rangle &\to \mathbb{C}[\wp_{gi}, \wp_{ggi}], \\ X_{gi} &\mapsto \wp_{gi}, \\ X_{ggi} &\mapsto \wp_{ggi} \end{aligned}$$

is well-defined and an isomorphism. In particular, we have the differential equations

$$F_i(\wp_{g1}, \wp_{g2}, \dots, \wp_{gg}, \wp_{gg1}, \wp_{gg2}, \dots, \wp_{ggg}) = 0.$$

Theorems 2.8 and 2.9 are proved similarly to [21, Chapter IIIa, Theorem 10.3]. In fact, when U_i and V_i are the coordinates of $J \setminus \Theta$ as in [21, Chapter IIIa, §1], we have

$$U_i = -\wp_{g,g-i+1}, \quad V_i = \frac{1}{2}\wp_{gg,g-i+1}$$

by Theorem 2.6.

Example 2.10. When $g = 1$, we have

$$F_1 = 4(X_{11}^3 + \lambda_2 X_{11}^2 + \lambda_1 X_{11} + \lambda_0) - X_{111}^2.$$

When $g = 2$, we have

$$\begin{aligned} F_1 &= 4X_{22}^4 + 4\lambda_4 X_{22}^3 + (12X_{12} + 4\lambda_3)X_{22}^2 + (8\lambda_4 X_{12} - X_{222}^2 + 4\lambda_2)X_{22} \\ &\quad + 4X_{12}^2 + 4\lambda_3 X_{12} - 2X_{122}X_{222} + 4\lambda_1, \\ F_2 &= 4X_{12}X_{22}^3 + 4\lambda_4 X_{12}X_{22}^2 + (8X_{12}^2 + 4\lambda_3 X_{12})X_{22} \\ &\quad + 4\lambda_4 X_{12}^2 + (-X_{222}^2 + 4\lambda_2)X_{12} - X_{122}^2 + 4\lambda_0. \end{aligned}$$

By Theorem 2.9, we can represent any meromorphic function on J with only pole along Θ as a polynomial in $\wp_{gi}$ and $\wp_{ggi}$. However, these expression may be complicated and it may be difficult to derive them. Hence we often use all the second and third derivatives $\wp_{11}, \wp_{12}, \dots, \wp_{gg}$ and $\wp_{111}, \wp_{112}, \dots, \wp_{ggg}$. In fact, these derivatives often appear in the formulas in the rest of this paper.

Example 2.11. In the case of genus 2, Grant [12] obtained the defining equations of $J \setminus \Theta$, where he used all the second and third derivatives $\wp_{11}$, $\wp_{12}$, $\wp_{22}$, $\wp_{111}$, $\wp_{112}$, $\wp_{122}$, $\wp_{222}$. We use his equations:

$$\begin{aligned}
F_3 &= X_{12}X_{222} - X_{122}X_{22} - X_{112},\\
F_4 &= 2(X_{22} + \lambda_4)X_{112} - (X_{12} + \lambda_3)X_{122} - X_{11}X_{222} - X_{111},\\
F_5 &= (4X_{22} + 4\lambda_4)X_{12}^2 - 4X_{11}X_{12} + 4\lambda_0 - X_{122}^2,\\
F_6 &= 4(X_{22}^3 + X_{12}X_{22} + \lambda_4 X_{22}^2 + X_{11} + \lambda_3 X_{22} + \lambda_2) - X_{222}^2,\\
F_7 &= 2X_{12}^2 + (4X_{22}^2 + 4\lambda_4 X_{22} + 2\lambda_3)X_{12} + 2\lambda_1 - 2X_{11}X_{22} - X_{122}X_{222}.
\end{aligned}$$

Note that our coordinates X_{ijk} are different from Grant's coordinates. We have the isomorphism

$$\begin{aligned}
\mathbb{C}[X_{ij}, X_{ijk}]/\langle F_3, F_4, \ldots, F_7\rangle &\to \mathbb{C}[\wp_{ij}, \wp_{ijk}],\\
X_{ij} &\mapsto \wp_{ij},\\
X_{ijk} &\mapsto \wp_{ijk}.
\end{aligned}$$

We can also obtain the defining equations like those in Example 2.11 in the case of genus 3. See [5, Theorem 4.7].

H. F. Baker [3] proved the following relation between $\wp_{ijkl}$ and $\wp_{ij}$.

Theorem 2.12 (Fundamental formula). *Let e_1, e_2, e_3, and e_4 be indeterminates. Let*

$$f(x,z) = \sum_{i=0}^{g} x^i z^i (\lambda_{2i+1}(x+z) + 2\lambda_{2i}),$$

where $\lambda_{2g+1} = 1$. Then we have

$$\begin{aligned}
&\prod_{1\le i<j\le 4}(e_i - e_j)\cdot \sum_{1\le i,j,k,l\le g} \wp_{ijkl}(u) e_1^{i-1}e_2^{j-1}e_3^{k-1}e_4^{l-1}\\
&= 2\sum_{\rho\in A_3}\Bigg[(e_{\rho(1)} - e_{\rho(2)})(e_4 - e_{\rho(3)})\\
&\cdot\left(f(e_{\rho(1)}, e_{\rho(2)}) - (e_{\rho(1)} - e_{\rho(2)})^2 \sum_{1\le i,j\le g}\wp_{ij}(u) e_{\rho(1)}^{i-1}e_{\rho(2)}^{j-1}\right)\\
&\cdot\left(f(e_4, e_{\rho(3)}) - (e_4 - e_{\rho(3)})^2 \sum_{1\le i,j\le g}\wp_{ij}(u) e_4^{i-1}e_{\rho(3)}^{j-1}\right)\Bigg],
\end{aligned} \tag{3}$$

where A_3 is the alternating group of degree 3.

Proof. See [3, pp. 136–144]. Note that our definition of the $\wp$-functions are different from that in [3] since the defining equation of C in [3] is taken as $y^2 = 4x^{2g+1} + \cdots$ while our defining equation is taken as $y^2 = x^{2g+1} + \cdots$. Therefore our formula also differs from that in [3, p. 144]. □

Corollary 2.13. *Let $1 \leq i, j, k, l \leq g$. Then $\wp_{ijkl}$ can be represented as a polynomial in $\wp_{11}, \wp_{12}, \ldots, \wp_{gg}$ with coefficients in $\mathbb{Z}[\lambda_i]$.*

Proof. The right-hand side of (3) is alternating with respect to $e_1, \ldots, e_4$. Hence it is divisible by $\prod(e_i - e_j)$. Since the coefficients of the right-hand side of (3) as a polynomial in $e_1, \ldots, e_4$ belong to $\mathbb{Z}[\lambda_i][\wp_{ij}]$, this corollary holds. □

Remark 2.14. Explicit descriptions of $\wp_{ijkl}$ in the case of genus 3 are written in [3, pp. 155–156] and [5, Section 4.2.2]. Note that our definition of $\wp$-functions is slightly different from theirs.

To describe the addition formula, we introduce the following functions:

$$\begin{aligned} m_{i,j}(u,v) = {} & \wp_{g,i+1}(u)\wp_{g,j+1}(v) - \wp_{g,i+1}(v)\wp_{g,j+1}(u) \\ & + \wp_{i,j+1}(v) - \wp_{i,j+1}(u) - \wp_{i+1,j}(v) + \wp_{i+1,j}(u), \end{aligned}$$

where we assume that $\wp_{mn} = 0$ unless $1 \leq m, n \leq g$. Let $k = g$ if g is even, $k = g + 1$ if g is odd. We define the skew-symmetric $k \times k$-matrix $M_g(u, v)$ by

$$M_g(u,v) = (m_{i,j}(u,v))_{0 \leq i,j \leq k-1}.$$

We denote the Pfaffian of the matrix $M_g(u, v)$ by $\mathcal{F}_g(u, v)$:

$$\mathcal{F}_g(u,v) = \operatorname{pf} M_g(u,v) = \sqrt{\det M_g(u,v)},$$

where the sign of the square root is chosen so that $\operatorname{pf} \left(\begin{smallmatrix} 0 & -1_n \\ 1_n & 0 \end{smallmatrix}\right) = (-1)^{n+1}$. Then $\mathcal{F}_g(u, v)$ is a polynomial in $\wp_{ij}(u)$ and $\wp_{ij}(v)$ with integral coefficients. We have the addition formula as follows:

Theorem 2.15 (Buchstaber-Enolskii-Leykin). *We have*

$$\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2} = \mathcal{F}_g(u,v).$$

Proof. See [6, Theorem 3.3]. □

Example 2.16. When $g = 1$, we have

$$\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2} = -\wp_{11}(u) + \wp_{11}(v).$$

This is a well-known formula (cf. [31, Chapter XX, p. 451, Example 1]).

When $g = 2$, we have

$$\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2} = -\wp_{11}(u) + \wp_{11}(v) - \wp_{12}(u)\wp_{22}(v) + \wp_{22}(u)\wp_{12}(v).$$

This formula is classical (cf. [4, p. 100]).

Finally, we review the result on the derivatives of the sigma function in [26]. For an integer n with $1 \leq n \leq g$, we denote by $\natural^n$ the set of positive integers i such that $n+1 \leq i \leq g$ and $i \equiv n+1 \pmod 2$, that is,

$$\natural^n = \begin{cases} \{n+1, n+3, \ldots, g\} & \text{if } g \equiv n+1 \pmod 2, \\ \{n+1, n+3, \ldots, g-1\} & \text{if } g \equiv n \pmod 2. \end{cases}$$

We also define $\sharp = \natural^1$ and $\flat = \natural^2$. For any meromorphic function F on $\mathbb{C}^g$, we define

$$F_{\natural^n}(u) = \left(\prod_{i \in \natural^n} \frac{\partial}{\partial u_i} \right) F(u).$$

Similarly, we define $F_\sharp = F_{\natural^1}$ and $F_\flat = F_{\natural^2}$. Note that $F_{\natural^g} = F$ since $\natural^g = \emptyset$.

Theorem 2.17 (Ônishi). *Let n be an integer with $1 \leq n \leq g$.*

(i) *Let $\check{\natural}^n$ be a proper subset of $\natural^n$ and*

$$\sigma_{\check{\natural}^n}(u) = \left(\prod_{i \in \check{\natural}^n} \frac{\partial}{\partial u_i} \right) \sigma(u).$$

Then $\sigma_{\check{\natural}^n}(u) = 0$ for any $u \in \kappa^{-1}(\Theta^{[n]})$.

(ii) *Let $u \in \kappa^{-1}(\Theta^{[n]})$. Then $\sigma_{\natural^n}(u) = 0$ if and only if $u \in \kappa^{-1}(\Theta^{[n-1]})$.*

Proof. (i) is [26, Lemma 6.2]. (ii) follows from [26, Proposition 6.5]. □

3. Division of hyperelliptic functions

In this section, we prove some lemmas on division of hyperelliptic functions. This section is technical, and the results in this section are only used to actually compute the division polynomials and to prove results on the coefficients of the division polynomials.

We use the theory of Gröbner bases in polynomial rings over Noetherian rings to prove the lemmas in this section. We do not include the definition and properties of Gröbner bases in this paper. For details, we refer the readers to [1, Chapter 4].

For simplicity, we restrict ourselves the case where the coefficient ring is a unique factorization domain (UFD). It is sufficient for our applications. We fix a term order on each polynomial ring throughout this section.

Definition 3.1. *Let R be a Noetherian UFD. Let $G = \{G_1, \ldots, G_t\}$ be a set of non-zero polynomials in $R[X_1, \ldots, X_n]$. Then we define*

$$\Delta(G) = \Delta(G_1, \ldots, G_t) = \operatorname{lcm}(\operatorname{lc}(G_i) \mid 1 \leq i \leq t)),$$

where $\operatorname{lc}(G_i)$ is the leading coefficient of G_i.

Lemma 3.2. *Let R be a Noetherian UFD and K be a field which contains R as a subring. Let $I \subset R[X_1, \ldots, X_n]$ be a non-zero ideal. Let G be a Gröbner basis for I. Then we have*

$$IK[X_1, \ldots, X_n] \cap R[X_1, \ldots, X_n] \\ = IR[1/\Delta(G)][X_1, \ldots, X_n] \cap R[X_1, \ldots, X_n].$$

Proof. If K is the quotient field of R, then the lemma follows from [1, Proposition 4.4.4] and the paragraph after the proof of it. For the general case, let F be the quotient field of R. Then K is an extension field of F. It is known that

$$IK[X_1, \ldots, X_n] \cap F[X_1, \ldots, X_n] = IF[X_1, \ldots, X_n],$$

which is clear by the theory of Gröbner bases, or see [29, §16.7, Lemma]. By taking the intersections of both sides and $R[X_1, \ldots, X_n]$, we obtain the lemma. □

Lemma 3.3. *Let R be a Noetherian UFD and K be a field which contains R as a subring. Let I be a non-zero ideal in $R[X_1, \ldots, X_n]$, $I_K = IK[X_1, \ldots, X_n]$, and $\pi\colon K[X_1, \ldots, X_n] \to K[X_1, \ldots, X_n]/I_K$ be the natural map. We assume that I_K is a prime ideal. Let $S \in R[X_1, \ldots, X_n]$ with $\pi(S) \neq 0$. Let G be a Gröbner basis for $I + \langle S \rangle$ and $\Delta = \Delta(G)$. Then, for any $P \in R[1/\Delta][X_1, \ldots, X_n]$ and any $Q \in K[X_1, \ldots, X_n]$ with $\pi(P) = \pi(QS)$, there exists $Q' \in R[1/\Delta][X_1, \ldots, X_n]$ such that $\pi(Q') = \pi(Q)$.*

Proof. By assumption, $P - QS \in I_K$. Hence we have $P \in I_K + \langle S \rangle$. Since $P \in R[1/\Delta][X_1, \ldots, X_n]$, there exists a non-negative integer m such that $\Delta^m P \in R[X_1, \ldots, X_n]$. Let $P' = \Delta^m P$. Then $P' \in (I_K + \langle S \rangle) \cap R[X_1, \ldots, X_n]$. By Lemma 3.2,

$$(I_K + \langle S \rangle) \cap R[X_1, \ldots, X_n] = (I + \langle S \rangle)R[1/\Delta][X_1, \ldots, X_n] \cap R[X_1, \ldots, X_n].$$

Therefore there exists $Q'' \in R[1/\Delta][X_1, \ldots, X_n]$ such that $P' - Q''S \in I_K$. Let $Q' = Q''/\Delta^m$. Then $P - Q'S \in I_K$, that is, $\pi(P) = \pi(Q'S)$. Since I_K is a prime ideal, we have $\pi(Q') = \pi(Q)$. □

By using Lemma 3.3, we can prove a lemma on division of hyperelliptic functions.

Lemma 3.4. *Let R be a Noetherian UFD which is a subring of $\mathbb{C}$ and which contains $\mathbb{Z}[\lambda_i]$. Let $S \in R[\wp_{gi}, \wp_{ggi}]$ be a non-zero function. Let $\tilde{S} \in R[X_{gi}, X_{ggi}]$ be a polynomial with $\tilde{S}(\wp_{gi}, \wp_{ggi}) = S$. Let G be a Gröbner basis for $\langle F_1, \ldots, F_g, \tilde{S} \rangle$ in $R[X_{gi}, X_{ggi}]$, where $F_1, \ldots, F_g$ are the polynomials in Theorem 2.9. Let $\Delta = \Delta(G)$. Then, for any $P \in R[1/\Delta][\wp_{gi}, \wp_{ggi}]$ and any $Q \in \mathbb{C}[\wp_{gi}, \wp_{ggi}]$, if $P = QS$, then $Q \in R[1/\Delta][\wp_{gi}, \wp_{ggi}]$.*

Proof. By Theorem 2.9, the homomorphism

$$\begin{aligned}\varphi\colon \mathbb{C}[X_{gi}, X_{ggi}]/\langle F_1, \dots, F_g\rangle &\to \mathbb{C}[\wp_{gi}, \wp_{ggi}],\\ X_{gi} &\mapsto \wp_{gi},\\ X_{ggi} &\mapsto \wp_{ggi}\end{aligned}$$

is an isomorphism. Since the right-hand side is an integral domain, $\langle F_1, \dots, F_g\rangle$ is a prime ideal. Therefore the lemma follows from Lemma 3.3. □

In Lemma 3.4, we use the defining equations of $J \setminus \Theta$ in Theorem 2.9. We can also use other defining equations of $J \setminus \Theta$. In the case of genus 2, we can use the defining equations in Example 2.11. Then we have the following lemma.

Lemma 3.5. *Let $g = 2$. Let R be a Noetherian UFD which is a subring of $\mathbb{C}$ and which contains $\mathbb{Z}[\lambda_i]$. Let $S \in R[\wp_{ij}, \wp_{ijk}]$ be a non-zero function. Let $\tilde{S} \in R[X_{ij}, X_{ijk}]$ be a polynomial with $\tilde{S}(\wp_{ij}, \wp_{ijk}) = S$. Let G be a Gröbner basis for $\langle F_3, \dots, F_7, \tilde{S}\rangle$ in $R[X_{ij}, X_{ijk}]$, where $F_3, \dots, F_7$ are the polynomials in Example 2.11. Let $\Delta = \Delta(G)$. Then, for any $P \in R[1/\Delta][\wp_{ij}, \wp_{ijk}]$ and any $Q \in \mathbb{C}[\wp_{ij}, \wp_{ijk}]$, if $P = QS$, then $Q \in R[1/\Delta][\wp_{ij}, \wp_{ijk}]$.*

The proof is similar to that of Lemma 3.4.

Remark 3.6. The denominator Δ in Lemma 3.4 or 3.5 depends on the term order and the choice of the Gröbner basis G.

4. The division polynomials

In this section, we define the division polynomials and study their properties. Our definition is a generalization of that in [15].

Definition 4.1. *For an integer n, we define the* division polynomial ϕ_n *by*

$$\phi_n(u) = \frac{\sigma(nu)}{\sigma(u)^{n^2}}. \tag{4}$$

Remark 4.2. For $g = 1$, the usual definition of the division polynomials is $\psi_n(u) = (-1)^{n+1}\sigma(nu)/\sigma(u)^{n^2}$.

Proposition 4.3. *For any integer n,*

$$\phi_{-n}(u) = \begin{cases} -\phi_n(u) & \text{if } g \equiv 1, 2 \pmod 4,\\ \phi_n(u) & \text{if } g \equiv 0, 3 \pmod 4.\end{cases}$$

Proof. The proposition immediately follows from Proposition 2.3. □

Proposition 4.4. *For any integer n, $\phi_n(u)$ is periodic with respect to Λ. Therefore it is a meromorphic function on J.*

Proof. The proposition follows from Proposition 2.2 by an easy calculation. □

By Proposition 4.4, we can write $\phi_n(P) = \phi_n(u)$ for $P = \kappa(u)$.

Corollary 4.5. *For any integer n, $\phi_n \in \mathbb{C}[\wp_{gi}, \wp_{ggi}]$.*

Proof. The function $\phi_n(u)$ has a pole only along Θ by definition. Therefore the corollary follows from Theorem 2.8. □

Remark 4.6. We will prove a stronger result later. See Theorem 5.8. However, we use Corollary 4.5 in the proof of it.

The following theorem describes a condition that a point in the Jacobian is an n-torsion point by the division polynomial and its derivatives.

Theorem 4.7. *Let n be a non-zero integer and $P \in J \setminus \Theta$. Then $[n]P = O$ if and only if $(\phi_n)_{\natural^m}(P) = 0$ for all $m = 1, 2, \ldots, g$.*

Proof. In the proof, we write

$$F_I(u) = \left(\prod_{i \in I} \frac{\partial}{\partial u_i}\right) F(u)$$

for a meromorphic function F and a subset $I \subset \natural^m$.

Let $u \in \mathbb{C}^g$ be a point with $\kappa(u) = P$. First, assume that $[n]P = O$. Then $nu \in \kappa^{-1}(\Theta^{[m]})$ for $0 \leq m \leq g$. Let $F(u) = 1/\sigma(u)^{n^2}$. Then $\phi_n(u) = \sigma(nu)F(u)$. Hence, for $1 \leq m \leq g$,

$$(\phi_n)_{\natural^m}(u) = \sum_{I \subset \natural^m} n^{|I|} \sigma_I(nu) F_{\natural^m \setminus I}(u), \tag{5}$$

where we denote by $|I|$ the number of elements in I. By Theorem 2.17, $\sigma_I(nu) = 0$ for any subset $I \subset \natural^m$. Therefore $(\phi_n)_{\natural^m}(P) = 0$.

Conversely, assume that $(\phi_n)_{\natural^m}(P) = 0$ for $m = 1, 2, \ldots, g$. It is sufficient to prove that $nu \in \kappa^{-1}(\Theta^{[m]})$ for $0 \leq m \leq g$. We prove it by induction on m. It is clear when $m = g$. Assume that $nu \in \kappa^{-1}(\Theta^{[m]})$. By Theorem 2.17 (i), for any proper subset $I \subsetneq \natural^m$, $\sigma_I(nu) = 0$. Therefore, by (5) and the assumption that $(\phi_n)_{\natural^m}(u) = 0$,

$$n^{|\natural^m|} \sigma_{\natural^m}(nu) F(u) = 0.$$

Since $F(u) \neq 0$, we have $\sigma_{\natural^m}(nu) = 0$. By Theorem 2.17 (ii), we have $nu \in \kappa^{-1}(\Theta^{[m-1]})$. □

Remark 4.8. When $g = 1$, Theorem 4.7 is clear and well-known. When $g = 2$, Kanayama [15, Theorem 7] proved that $[n]P = O$ if and only if $\phi_n(P) = (\partial\phi_n/\partial u_2)(P) = (\partial^2\phi_n/\partial u_2^2)(P) = 0$. Since $(\phi_n)_{\natural^2} = \phi_n$ and $(\phi_n)_{\natural^1} = \partial\phi_n/\partial u_2$, Theorem 4.7 is a refinement of Kanayama's result.

As generalizations of Kanayama's results [15, Proposition 1 and Lemma 1], we have the following propositions.

Proposition 4.9. *Let m and n be integers. Then we have*

$$\frac{\phi_{m+n}(u)\phi_{m-n}(u)}{\phi_m(u)^2\phi_n(u)^2} = \mathcal{F}_g(mu, nu) \quad (m, n \neq 0), \tag{6}$$

$$\phi_{mn}(u) = \phi_m(nu)\phi_n(u)^{m^2}. \tag{7}$$

Proof. These formulas easily follow from Theorem 2.15 and the definition of the division polynomials. □

Proposition 4.10. *Let n be a non-zero integer. Then we have*

$$\wp_{ij}(nu) = \wp_{ij}(u) + \frac{\phi_n^{(i)}\phi_n^{(j)} - \phi_n\phi_n^{(ij)}}{n^2\phi_n^2},$$

$$\wp_{ijk}(nu) = \frac{1}{n}\wp_{ijk}(u) - \frac{\phi_n^{(ijk)}\phi_n^2 - \left(\phi_n^{(ij)}\phi_n^{(k)} + \phi_n^{(ki)}\phi_n^{(j)} + \phi_n^{(jk)}\phi_n^{(i)}\right)\phi_n + 2\phi_n^{(i)}\phi_n^{(j)}\phi_n^{(k)}}{n^3\phi_n^3},$$

where $\phi_n = \phi_n(u)$, $\phi_n^{(i)} = \partial\phi_n/\partial u_i$, $\phi_n^{(ij)} = \partial\phi_n^{(i)}/\partial u_j$, $\phi_n^{(ijk)} = \partial\phi_n^{(ij)}/\partial u_k$.

Proof. Take the logarithmic derivatives of both sides of (4). □

For $n = 0, 1, 2$, the division polynomial ϕ_n is described as follows:

Theorem 4.11. *We have*

$$\phi_0(u) = 0, \quad \phi_1(u) = 1,$$

$$\phi_2(u) = \left.\frac{\partial^l \mathcal{F}_g(v, u)}{\partial v_1 \partial v_3 \dots \partial v_{2l-1}}\right|_{v=u},$$

where $g = 2l - 1$ or $g = 2l$. In particular, $\phi_0(u), \phi_1(u), \phi_2(u) \in \mathbb{Z}[\lambda_i][\wp_{ij}, \wp_{ijk}]$.

For the proof, we need an analog of de l'Hôpital's rule.

Lemma 4.12. *Let $D \subset \mathbb{C}^g$ be a domain and $\alpha \in D$. Let F and G be holomorphic functions on D. Assume that F/G can be extended as a holomorphic function H on D. Let*

$$d = \min\left\{ n \in \mathbb{Z}_{\geq 0} \;\middle|\; \text{there exist } i_1, \dots, i_n \text{ such that } \frac{\partial^n G}{\partial u_{i_1} \cdots \partial u_{i_n}}(\alpha) \neq 0 \right\}.$$

Then, if indices $i_1, \dots, i_d$ satisfy $(\partial^d G/\partial u_{i_1} \dots \partial u_{i_d})(\alpha) \neq 0$, we have

$$\lim_{\substack{u \to \alpha \\ G(u) \neq 0}} \frac{F(u)}{G(u)} = \frac{(\partial^d F/\partial u_{i_1} \dots \partial u_{i_d})(\alpha)}{(\partial^d G/\partial u_{i_1} \dots \partial u_{i_d})(\alpha)} = H(\alpha).$$

Proof. Let $S = \{1, 2, \dots, d\}$. For simplicity, we write

$$F_I(u) = \left(\prod_{j \in I} \frac{\partial}{\partial u_{i_j}} \right) F(u)$$

for any subset $I \subset S$.

Since $F(u) = G(u)H(u)$, we have

$$F_S(u) = \sum_{I \subset S} G_I(u) H_{S \setminus I}(u).$$

If I is a proper subset of S, then $G_I(\alpha) = 0$ by the definition of d. Hence we have

$$F_S(\alpha) = G_S(\alpha) H(\alpha).$$

This proves the lemma. □

Proof (Proof of Theorem 4.11). We have $\phi_0(u) = 0$ and $\phi_1(u) = 1$ by definition.

By Theorem 2.15,

$$\frac{\sigma(u+v)}{\sigma(u)^2 \sigma(v)^2} = \frac{\mathcal{F}_g(v,u)}{\sigma(v-u)}. \tag{8}$$

If we fix u, then the left-hand side of (8) is holomorphic with respect to v in a neighborhood of $v = u$. By Proposition 2.1,

$$\left. \frac{\partial^l \sigma(v-u)}{\partial v_1 \partial v_3 \dots \partial v_{2l-1}} \right|_{v=u} = 1.$$

Therefore, by Lemma 4.12,

$$\phi_2(u) = \frac{\sigma(2u)}{\sigma(u)^4} = \left. \frac{\partial^l \mathcal{F}_g(v,u)}{\partial v_1 \partial v_3 \dots \partial v_{2l-1}} \right|_{v=u}.$$

Since $\mathcal{F}_g(u,v)$ is a polynomial in $\wp_{ij}(u)$ and $\wp_{ij}(v)$ with integral coefficients, by Corollary 2.13, we have $\phi_2(u) \in \mathbb{Z}[\lambda_i][\wp_{ij}, \wp_{ijk}]$. □

Example 4.13. For $g = 1$, we have

$$\phi_2(u) = \wp_{11}(u).$$

For $g = 2$, we have

$$\phi_2(u) = \wp_{12}(u)\wp_{122}(u) - \wp_{22}(u)\wp_{112}(u) - \wp_{111}(u).$$

Now we can compute the division polynomial ϕ_n by Lemma 3.4, Propositions 4.9 and 4.10, and Theorem 4.11 as in [15, pp. 403–404]. Although we can use determinantal expressions (Theorems 5.5 and 5.7) or the recurrence formula (Theorem 6.4), they are rather complicated for $g \geq 2$.

For $g = 2$ and $1 \leq n \leq 5$, the author computed ϕ_n and verified that $\phi_n \in \mathbb{Z}[\lambda_i][\wp_{ij}, \wp_{ijk}]$ by using Maxima [19] and Risa/Asir [23]. Note that it is not necessary to use Lemma 3.4 in the case of genus 2 (see [15]). This fact suggests the following conjecture:

Conjecture 4.14. For any integer n, $\phi_n(u) \in \mathbb{Z}[\lambda_i][\wp_{ij}, \wp_{ijk}]$.

This conjecture is true for $g = 1$ (cf. [27, Section 1.3]). In the case of genus 2, Kanayama proved that $\phi_n \in \mathbb{Q}[\lambda_i][\wp_{ij}, \wp_{ijk}]$ for any integer n in [16, Corollary 1 (Corrected)]. We will prove a weaker result than Conjecture 4.14 in Theorem 5.8. Using Theorem 5.8, we will prove that $\phi_n \in \mathbb{Z}[1/2, \lambda_i][\wp_{ij}, \wp_{ijk}]$ for $g = 2$ in Example 5.9. This statement is stronger than Kanayama's result.

5. Determinantal expressions

In this section, we give determinantal expressions for the division polynomial ϕ_n. As an application, we prove a result on the coefficients of ϕ_n as a polynomial in the $\wp$-functions.

Let $u \in \kappa^{-1}(\Theta^{[1]})$. We define

$$w_0(u) = 1, \quad w_1(u) = x(u), \quad w_2(u) = x(u)^2, \quad \dots, \quad w_g(u) = x(u)^g,$$

and

$$w_{g+i}(u) = \begin{cases} x(u)^{(i-1)/2} y(u) & \text{if } i \text{ is odd,} \\ x(u)^{g+i/2} & \text{if } i \text{ is even,} \end{cases}$$

for $i \geq 1$. Ônishi proved the following formula.

Theorem 5.1 (Frobenius-Stickelberger-type formula). *Let n be an integer and $u^{(1)}, \dots, u^{(n)} \in \kappa^{-1}(\Theta^{[1]})$.*

(i) *If $2 \leq n \leq g$, then we have*

$$(-1)^{n(n-1)(n+g+1)/2} \frac{\sigma_\natural{}^n(u^{(1)} + \cdots + u^{(n)}) \prod_{1 \leq i < j \leq n} \sigma_\flat(u^{(i)} - u^{(j)})}{\sigma_\sharp(u^{(1)})^n \dots \sigma_\sharp(u^{(n)})^n} = \det\left(w_{j-1}(u^{(i)})\right)_{1 \leq i,j \leq n}.$$

(ii) *If $n \geq g$, then we have*

$$(-1)^{(n-g-1)(n+g^2+2g)/2} \frac{\sigma(u^{(1)} + \cdots + u^{(n)}) \prod_{1 \leq i < j \leq n} \sigma_\flat(u^{(i)} - u^{(j)})}{\sigma_\sharp(u^{(1)})^n \dots \sigma_\sharp(u^{(n)})^n} = \det\left(w_{j-1}(u^{(i)})\right)_{1 \leq i,j \leq n}.$$

Remark 5.2. Theorem 5.1 is proved in [26, Theorem 8.2]. Unfortunately, the sign in [26, Theorem 8.2] is incorrect since the sign in [26, Proposition 5.1] is miscalculated. The sign $(-1)^{g(g-1)(g-3)/2}$ in [26, Proposition 5.1] should be replaced by $(-1)^{g(g-2)(g-3)/2}$, then [26, Theorem 8.2] is modified as above.

Using Theorem 5.1, Ônishi also proved a similar formula for his division polynomial $\psi_n(u) = \sigma(nu)/\sigma_\sharp(u)^{n^2}$ (cf. [26, Theorem 9.3]). This formula is called the Kiepert-type formula. We prove a similar formula for our division polynomial $\phi_n(u) = \sigma(nu)/\sigma(u)^{n^2}$.

We need some lemmas.

Lemma 5.3. *Fix an integer k with $1 \leq k \leq g$. Let u and v be on $\kappa^{-1}(\Theta^{[1]})$. Then*

$$\lim_{u \to v} \frac{\sigma_{\mathfrak{b}}(u-v)}{u_k - v_k} = \frac{1}{x^{k-1}(v)}.$$

Proof. See [26, Lemma 9.1]. □

Lemma 5.4. *For any genus g, the function $\sigma_{\mathfrak{b}}(u)$ is an odd function.*

Proof. Let $|\mathfrak{b}|$ be the number of elements in $\mathfrak{b}$. Then $|\mathfrak{b}|$ is $(g-1)/2$ if g is odd, and $(g-2)/2$ if g is even. Hence $|\mathfrak{b}|$ is an even number if $g \equiv 1, 2 \pmod 4$, and an odd number if $g \equiv 0, 3 \pmod 4$. Therefore the lemma follows from Proposition 2.3. □

Using these lemmas, we prove the following theorem.

Theorem 5.5 (Kiepert-type formula). *Fix an integer k with $1 \leq k \leq g$. Let $n \geq 1$ be an integer, $u^{(1)}, \dots, u^{(g)} \in \kappa^{-1}(\Theta^{[1]})$, and $u = u^{(1)} + \cdots + u^{(g)}$. We define*

$$N_n(u^{(1)}, \dots, u^{(g)}) = \begin{vmatrix} 1 & w_1(u^{(1)}) & w_2(u^{(1)}) & \dots & w_{ng-1}(u^{(1)}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w_1(u^{(g)}) & w_2(u^{(g)}) & \dots & w_{ng-1}(u^{(g)}) \\ 0 & w_1'(u^{(1)}) & w_2'(u^{(1)}) & \dots & w_{ng-1}'(u^{(1)}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & w_1'(u^{(g)}) & w_2'(u^{(g)}) & \dots & w_{ng-1}'(u^{(g)}) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & w_1^{(n-1)}(u^{(1)}) & w_2^{(n-1)}(u^{(1)}) & \dots & w_{ng-1}^{(n-1)}(u^{(1)}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & w_1^{(n-1)}(u^{(g)}) & w_2^{(n-1)}(u^{(g)}) & \dots & w_{ng-1}^{(n-1)}(u^{(g)}) \end{vmatrix}$$

and

$$D(u^{(1)}, \dots, u^{(g)}) = \begin{vmatrix} 1 & w_1(u^{(1)}) & w_2(u^{(1)}) & \dots & w_{g-1}(u^{(1)}) \\ 1 & w_1(u^{(2)}) & w_2(u^{(2)}) & \dots & w_{g-1}(u^{(2)}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w_1(u^{(g)}) & w_2(u^{(g)}) & \dots & w_{g-1}(u^{(g)}) \end{vmatrix},$$

where the symbols $', '', \dots, {}^{(n-1)}$ denote

$$\frac{d}{du_k}, \quad \left(\frac{d}{du_k}\right)^2, \quad \dots, \left(\frac{d}{du_k}\right)^{n-1}$$

respectively. Here we regard $w_j(u)$ locally as a function of u_k. Then we have

$$\phi_n(u) = \varepsilon_n \frac{\left(x(u^{(1)}) \cdots x(u^{(g)})\right)^{(k-1)n(n-1)/2} N_n(u^{(1)}, \dots, u^{(g)})}{(1!2! \cdots (n-1)!)^g D(u^{(1)}, \dots, u^{(g)})^{n^2}},$$

where

$$\varepsilon_n = \begin{cases} 1 & \text{if } g \equiv 0 \pmod 4, \\ (-1)^{n-1} & \text{if } g \equiv 1 \pmod 4, \\ (-1)^{n(n-1)/2} & \text{if } g \equiv 2,3 \pmod 4. \end{cases} \tag{9}$$

Proof. We divide the proof into two steps. The first step is taking limits of both sides of the Frobenius-Stickelberger-type formula (Theorem 5.1). This step is similar to the proof of Ônishi's Kiepert-type formula ([24, Theorem 3.3]). The second step is eliminating $\sigma_\sharp$ and $\sigma_\flat$ by combining the formula obtained in the first step and the Frobenius-Stickelberger-type formula itself.

Step 1. Replacing n by ng in Theorem 5.1, we have

$$(-1)^{g(ng-g-1)(n+g+2)/2} \frac{\sigma(u^{(1)} + \cdots + u^{(ng)}) \prod_{1 \le i < j \le ng} \sigma_\flat(u^{(i)} - u^{(j)})}{\sigma_\sharp(u^{(1)})^{ng} \dots \sigma_\sharp(u^{(ng)})^{ng}} = \begin{vmatrix} 1 & w_1(u^{(1)}) & w_2(u^{(1)}) & \dots & w_{ng-1}(u^{(1)}) \\ 1 & w_1(u^{(2)}) & w_2(u^{(2)}) & \dots & w_{ng-1}(u^{(2)}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w_1(u^{(ng)}) & w_2(u^{(ng)}) & \dots & w_{ng-1}(u^{(ng)}) \end{vmatrix}. \tag{10}$$

The right-hand side is equal to

$$\begin{vmatrix} 1 & w_1(u^{(1)}) & \dots & w_{ng-1}(u^{(1)}) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & w_1(u^{(g)}) & \dots & w_{ng-1}(u^{(g)}) \\ 0 & w_1(u^{(g+1)}) - w_1(u^{(1)}) & \dots & w_{ng-1}(u^{(g+1)}) - w_{ng-1}(u^{(1)}) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & w_1(u^{(2g)}) - w_1(u^{(g)}) & \dots & w_{ng-1}(u^{(2g)}) - w_{ng-1}(u^{(g)}) \\ 1 & w_1(u^{(2g+1)}) & \dots & w_{ng-1}(u^{(2g+1)}) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & w_1(u^{(ng)}) & \dots & w_{ng-1}(u^{(ng)}) \end{vmatrix}.$$

For $1 \le i \le g$, we put $h^{(i)} = u_k^{(g+i)} - u_k^{(i)}$. By Taylor's theorem,

$$w_j(u^{(g+i)}) - w_j(u^{(i)}) = w_j'(u^{(i)})h^{(i)} + (d^\circ(h^{(i)}) \ge 2).$$

Therefore, by dividing both sides of (10) by $h^{(1)}h^{(2)}\cdots h^{(g)}$, taking limits $u^{(g+i)} \to u^{(i)}$ for $1 \leq i \leq g$, and using Lemmas 5.3 and 5.4, we have

$$
\begin{aligned}
&(-1)^{g(ng-g-1)(n+g+2)/2+g+g(g-1)/2}\sigma(2u+u^{(2g+1)}+\cdots+u^{(ng)})\\
&\cdot \prod_{1\leq i<j\leq g}\sigma_\flat(u^{(i)}-u^{(j)})^4 \cdot \prod_{\substack{1\leq i\leq g\\ 2g+1\leq j\leq ng}}\sigma_\flat(u^{(i)}-u^{(j)})^2 \cdot \prod_{2g+1\leq i<j\leq ng}\sigma_\flat(u^{(i)}-u^{(j)})\\
&\Big/ \left(\prod_{i=1}^{g}\left(x(u^{(i)})^{k-1}\sigma_\sharp(u^{(i)})^{2ng}\right)\cdot \sigma_\sharp(u^{(2g+1)})^{ng}\cdots\sigma_\sharp(u^{(ng)})^{ng}\right)\\
&\qquad = \begin{vmatrix}
1 & w_1(u^{(1)}) & w_2(u^{(1)}) & \dots & w_{ng-1}(u^{(1)})\\
\vdots & \vdots & \vdots & \ddots & \vdots\\
1 & w_1(u^{(g)}) & w_2(u^{(g)}) & \dots & w_{ng-1}(u^{(g)})\\
0 & w_1'(u^{(1)}) & w_2'(u^{(1)}) & \dots & w_{ng-1}'(u^{(1)})\\
\vdots & \vdots & \vdots & \ddots & \vdots\\
0 & w_1'(u^{(g)}) & w_2'(u^{(g)}) & \dots & w_{ng-1}'(u^{(g)})\\
1 & w_1(u^{(2g+1)}) & w_2(u^{(2g+1)}) & \dots & w_{ng-1}(u^{(2g+1)})\\
\vdots & \vdots & \vdots & \ddots & \vdots\\
1 & w_1(u^{(ng)}) & w_2(u^{(ng)}) & \dots & w_{ng-1}(u^{(ng)})
\end{vmatrix}. \qquad (11)
\end{aligned}
$$

We repeat these operations. For $1 \leq i \leq g$, we put $h^{(i)} = u_k^{(2g+i)} - u_k^{(i)}$. The right-hand side of (11) is equal to

$$
\begin{vmatrix}
1 & w_1(u^{(1)}) & \dots\\
\vdots & \vdots & \ddots\\
1 & w_1(u^{(g)}) & \dots\\
0 & w_1'(u^{(1)}) & \dots\\
\vdots & \vdots & \ddots\\
0 & w_1'(u^{(g)}) & \dots\\
0 & w_1(u^{(2g+1)}) - w_1(u^{(1)}) - w_1'(u^{(1)})h^{(1)} & \dots\\
\vdots & \vdots & \ddots\\
0 & w_1(u^{(3g)}) - w_1(u^{(g)}) - w_1'(u^{(1)})h^{(g)} & \dots\\
1 & w_1(u^{(3g+1)}) & \dots\\
\vdots & \vdots & \ddots\\
1 & w_1(u^{(ng)}) & \dots
\end{vmatrix}.
$$

By Taylor's theorem,

$$
w_j(u^{(g+i)}) - w_j(u^{(i)}) - w_j'(u^{(i)})h^{(i)} = \frac{1}{2!}w_j''(u^{(i)})(h^{(i)})^2 + (d^\circ(h^{(i)}) \geq 3).
$$

Therefore, by dividing both sides of (11) by $\left(h^{(1)}h^{(2)}\cdots h^{(g)}\right)^2$, taking limits $u^{(2g+i)} \to u^{(i)}$ for $1 \le i \le g$, and using Lemmas 5.3 and 5.4, we have

$$(-1)^{g(ng-g-1)(n+g+2)/2+(1+2)(g+g(g-1)/2)}\sigma(3u+u^{(3g+1)}+\cdots+u^{(ng)})$$
$$\cdot \prod_{1\le i<j\le g}\sigma_\flat(u^{(i)}-u^{(j)})^9 \cdot \prod_{\substack{1\le i\le g\\ 3g+1\le j\le ng}}\sigma_\flat(u^{(i)}-u^{(j)})^3 \cdot \prod_{3g+1\le i<j\le ng}\sigma_\flat(u^{(i)}-u^{(j)})$$
$$\Big/ \left(\prod_{i=1}^{g}\left(x(u^{(i)})^{3(k-1)}\sigma_\sharp(u^{(i)})^{3ng}\right)\cdot \sigma_\sharp(u^{(3g+1)})^{ng}\cdots\sigma_\sharp(u^{(ng)})^{ng}\right)$$
$$= \frac{1}{(2!)^g}\begin{vmatrix} 1 & w_1(u^{(1)}) & w_2(u^{(1)}) & \dots & w_{ng-1}(u^{(1)}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w_1(u^{(g)}) & w_2(u^{(g)}) & \dots & w_{ng-1}(u^{(g)}) \\ 0 & w_1'(u^{(1)}) & w_2'(u^{(1)}) & \dots & w_{ng-1}'(u^{(1)}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & w_1'(u^{(g)}) & w_2'(u^{(g)}) & \dots & w_{ng-1}'(u^{(g)}) \\ 0 & w_1''(u^{(1)}) & w_2''(u^{(1)}) & \dots & w_{ng-1}''(u^{(1)}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & w_1''(u^{(g)}) & w_2''(u^{(g)}) & \dots & w_{ng-1}''(u^{(g)}) \\ 1 & w_1(u^{(3g+1)}) & w_2(u^{(3g+1)}) & \dots & w_{ng-1}(u^{(3g+1)}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w_1(u^{(ng)}) & w_2(u^{(ng)}) & \dots & w_{ng-1}(u^{(ng)}) \end{vmatrix}.$$

Repeating these operations, we have

$$(-1)^\alpha \frac{\sigma(nu)\prod_{1\le i<j\le g}\sigma_\flat(u^{(i)}-u^{(j)})^{n^2}}{\prod_{i=1}^{g}\left(x(u^{(i)})^{(k-1)n(n-1)/2}\sigma_\sharp(u^{(i)})^{n^2g}\right)} = \frac{1}{(1!2!\cdots(n-1)!)^g}N_n(u^{(1)},\dots,u^{(g)}), \quad (12)$$

where

$$\alpha = \frac{1}{2}g(ng-g-1)(n+g+2) + \left(1+2+\cdots+(n-1)\right)\left(g+\frac{1}{2}g(g-1)\right)$$
$$= \frac{1}{2}g(ng-g-1)(n+g+2) + \frac{1}{4}n(n-1)g(g+1).$$

Step 2. Replacing n by g in Theorem 5.1, we have

$$(-1)^{g(g-1)/2}\frac{\sigma(u)\prod_{1\le i<j\le g}\sigma_\flat(u^{(i)}-u^{(j)})}{\prod_{i=1}^{g}\sigma_\sharp(u^{(i)})^g} = D(u^{(1)},\dots,u^{(g)}). \quad (13)$$

Combining (12) and (13), we have

$$\phi_n(u) = \varepsilon_n \frac{\left(x(u^{(1)})\cdots x(u^{(g)})\right)^{(k-1)n(n-1)/2}N_n(u^{(1)},\dots,u^{(g)})}{(1!2!\cdots(n-1)!)^g D(u^{(1)},\dots,u^{(g)})^{n^2}},$$

where

$$\varepsilon_n = (-1)^{\beta},$$
$$\beta = \frac{1}{2}g(ng-g-1)(n+g+2) + \frac{1}{4}n(n-1)g(g+1) - \frac{1}{2}n^2g(g-1).$$

It is easy to verify that ε_n satisfies (9). □

In Theorem 5.5, we use derivatives with respect to u_k. By using derivatives with respect to x, we obtain another formula.

Let $\mu(u)$ be a function on $\kappa^{-1}(\Theta^{[1]})$. We denote by $\dot{\mu}(u)$, $\ddot{\mu}(u)$, …, $\mu^{\langle\nu\rangle}(u)$ the functions

$$\frac{d\mu}{dx}(u), \quad \frac{d^2\mu}{dx^2}(u), \quad \ldots, \frac{d^\nu\mu}{dx^\nu}(u)$$

respectively.

Lemma 5.6. *Let $m > 0$ be any integer. Then we have*

$$\frac{1}{m!}\big(2y(u)\big)^{2m-1}y^{\langle m\rangle}(u) \in \mathbb{Z}[\lambda_i][x(u), y(u)].$$

Proof. We prove the lemma by induction on m. Since $\dot{y}(u) = \dot{f}(x(u))/\big(2y(u)\big)$, the lemma holds for $m = 1$.

We assume that the lemma holds for 1, 2, …, $m-1$. Then, for any integer $1 \leq k \leq m-1$, there exists $a_k(u) \in \mathbb{Z}[\lambda_i][x(u), y(u)]$ such that $y^{\langle k\rangle}(u) = k!a_k(u)/\big(2y(u)\big)^{2k-1}$. By differentiating the defining equation $y^2 = f(x)$, we have

$$2y(u)y^{\langle m\rangle}(u) = f^{\langle m\rangle}(x(u)) - \sum_{k=1}^{m-1}\binom{m}{k}y^{\langle k\rangle}(u)y^{\langle m-k\rangle}(u).$$

It is easily seen that $f^{\langle m\rangle}(x(u))/m! \in \mathbb{Z}[\lambda_i][x(u)]$. By assumption, we have

$$\binom{m}{k}y^{\langle k\rangle}(u)y^{\langle m-k\rangle}(u) = m!\frac{a_k(u)a_{m-k}(u)}{\big(2y(u)\big)^{2m-2}}.$$

Therefore the lemma holds for m. □

For integers $i, j \geq 0$, we define

$$W_{i,j}(u) = \frac{w_j^{\langle i\rangle}(u)}{i!}.$$

Then we have the following formula.

Theorem 5.7. *Under the assumptions and notation of Theorem 5.5, we define*

$$M_n(u^{(1)},\dots,u^{(g)}) = \begin{vmatrix} W_{0,0}(u^{(1)}) & W_{0,1}(u^{(1)}) & \dots & W_{0,ng-1}(u^{(1)}) \\ \vdots & \vdots & \ddots & \vdots \\ W_{0,0}(u^{(g)}) & W_{0,1}(u^{(g)}) & \dots & W_{0,ng-1}(u^{(g)}) \\ W_{1,0}(u^{(1)}) & W_{1,1}(u^{(1)}) & \dots & W_{1,ng-1}(u^{(1)}) \\ \vdots & \vdots & \ddots & \vdots \\ W_{1,0}(u^{(g)}) & W_{1,1}(u^{(g)}) & \dots & W_{1,ng-1}(u^{(g)}) \\ \vdots & \vdots & \vdots & \vdots \\ W_{n-1,0}(u^{(1)}) & W_{n-1,1}(u^{(1)}) & \dots & W_{n-1,ng-1}(u^{(1)}) \\ \vdots & \vdots & \ddots & \vdots \\ W_{n-1,0}(u^{(g)}) & W_{n-1,1}(u^{(g)}) & \dots & W_{n-1,ng-1}(u^{(g)}) \end{vmatrix}$$

and

$$F_n(u^{(1)},\dots,u^{(g)}) = \varepsilon_n\big(2^g y(u^{(1)})\cdots y(u^{(g)})\big)^{n(n-1)/2} M_n(u^{(1)},\dots,u^{(g)}).$$

Then we have

$$\phi_n(u) = \frac{F_n(u^{(1)},\dots,u^{(g)})}{D(u^{(1)},\dots,u^{(g)})^{n^2}}. \tag{14}$$

Furthermore we have

$$F_n(u^{(1)},\dots,u^{(g)}) \in \mathbb{Z}[\lambda_i][x(u^{(1)}),\dots,x(u^{(g)}),y(u^{(1)}),\dots,y(u^{(g)})]. \tag{15}$$

Proof. The proof of (14) is similar to that of Theorem 5.5. We omit the details.

We prove (15). To simplify notation, we write

$$R = \mathbb{Z}[\lambda_i][x(u^{(1)}),\dots,x(u^{(g)}),y(u^{(1)}),\dots,y(u^{(g)})].$$

Let s be the largest integer not exceeding $(n-1)g/2$, and $r = ng-s$. By (14), we have

$$\phi_n(u) = \pm\frac{\big(2^g y(u^{(1)})\cdots y(u^{(g)})\big)^{n(n-1)/2}}{D(u^{(1)},\dots,u^{(g)})^{n^2}} \cdot \begin{vmatrix} \frac{1}{0!} & \frac{x(u^{(1)})}{0!} & \dots & \frac{x^{r-1}(u^{(1)})}{0!} & \frac{y(u^{(1)})}{0!} & \dots & \frac{(x^{s-1}y)(u^{(1)})}{0!} \\ 0 & \frac{\dot{x}(u^{(1)})}{1!} & \dots & \frac{(x^{r-1})^{\langle 1\rangle}(u^{(1)})}{1!} & \frac{\dot{y}(u^{(1)})}{1!} & \dots & \frac{(x^{s-1}y)^{\langle 1\rangle}(u^{(1)})}{1!} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \frac{x^{\langle n-1\rangle}(u^{(1)})}{(n-1)!} & \dots & \frac{(x^{r-1})^{\langle n-1\rangle}(u^{(1)})}{(n-1)!} & \frac{y^{\langle n-1\rangle}(u^{(1)})}{(n-1)!} & \dots & \frac{(x^{s-1}y)^{\langle n-1\rangle}(u^{(1)})}{(n-1)!} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \frac{1}{0!} & \frac{x(u^{(g)})}{0!} & \dots & \frac{x^{r-1}(u^{(g)})}{0!} & \frac{y(u^{(g)})}{0!} & \dots & \frac{(x^{s-1}y)(u^{(g)})}{0!} \\ 0 & \frac{\dot{x}(u^{(g)})}{1!} & \dots & \frac{(x^{r-1})^{\langle 1\rangle}(u^{(g)})}{1!} & \frac{\dot{y}(u^{(g)})}{1!} & \dots & \frac{(x^{s-1}y)^{\langle 1\rangle}(u^{(g)})}{1!} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \frac{x^{\langle n-1\rangle}(u^{(g)})}{(n-1)!} & \dots & \frac{(x^{r-1})^{\langle n-1\rangle}(u^{(g)})}{(n-1)!} & \frac{y^{\langle n-1\rangle}(u^{(g)})}{(n-1)!} & \dots & \frac{(x^{s-1}y)^{\langle n-1\rangle}(u^{(g)})}{(n-1)!} \end{vmatrix}.$$

Let A be the matrix in the right-hand side. We denote by $A^{i_1\dots i_k}_{j_1\dots j_k}$ the submatrix of A consisting of the rows $i_1,\dots,i_k$ and the columns $j_1,\dots,j_k$. By the Laplace expansion,

$$\det A = \sum_{1\le i_1<\cdots<i_r\le ng} (-1)^{i_1+\cdots+i_r+r(r+1)/2} |A|^{i_1\dots i_r}_{1\dots r} |A|^{i_{r+1}\dots i_{ng}}_{r+1\dots ng},$$

where $i_{r+1},\dots,i_{ng}$ are the indices with $i_{r+1}<\cdots<i_{ng}$ and $\{i_1,\dots,i_{ng}\}=\{1,\dots,ng\}$. Since each entry of $A^{i_1\dots i_r}_{1\dots r}$ is of the form $(x^l)^{\langle m\rangle}(u^{(k)})/m!$, we have $|A|^{i_1\dots i_r}_{1\dots r}\in R$. Therefore it is sufficient to prove that

$$\left(2^g y(u^{(1)})\cdots y(u^{(g)})\right)^{n(n-1)/2} |A|^{i_{r+1}\dots i_{ng}}_{r+1\dots ng} \in R$$

for any $i_{r+1}<\cdots<i_{ng}$.

Fix indices $i_{r+1}<\cdots<i_{ng}$ and let $B=A^{i_{r+1}\dots i_{ng}}_{r+1\dots ng}$. For $1\le k\le g$, let t_k be the number of the rows containing the variable $u^{(k)}$. We define $T_0=0$ and $T_k=t_1+\cdots+t_k$ for $1\le k\le g$. By using the Laplace expansion repeatedly,

$$\det B = \sum_{j_1,\dots,j_s} \varepsilon_{j_1,\dots,j_s} \prod_{k=1}^{g} |B|^{T_{k-1}+1\dots T_k}_{j_{T_{k-1}+1}\dots j_{T_k}},$$

where $j_1,\dots,j_s$ run through all indices satisfying that $\{j_1,\dots,j_s\}=\{1,\dots,s\}$ and $j_{T_{k-1}+1}<\cdots<j_{T_k}$ for all $1\le k\le g$. Here $\varepsilon_{j_1,\dots,j_s}=\pm1$. Then, for any $1\le k\le g$, $B^{T_{k-1}+1\dots T_k}_{j_{T_{k-1}+1}\dots j_{T_k}}$ is of the form

$$\left(\frac{(x^{l_j}y)^{\langle m_i\rangle}(u^{(k)})}{m_i!}\right)_{1\le i,j\le t_k},$$

where $0\le m_1\le\cdots\le m_{t_k}\le n-1$ and $0\le l_1\le\cdots\le l_{t_k}$. Therefore it is sufficient to prove the following claim:

Claim. Let $v\in\kappa^{-1}(\Theta^{[1]})$. Let $t\le n$ be a positive integer. Let $0\le m_1<\cdots<m_t\le n-1$ and $0\le l_1<\cdots<l_t$. Then we have

$$(2y(v))^{n(n-1)/2}\det\left(\frac{(x^{l_j}y)^{\langle m_i\rangle}(v)}{m_i!}\right)_{1\le i,j\le t}\in\mathbb{Z}[\lambda_i][x(v),y(v)].$$

First note that

$$\frac{(x^{l_j}y)^{\langle m_i\rangle}}{m_i!}=\sum_{k=0}^{m_i}\frac{(x^{l_j})^{\langle k\rangle}}{k!}\cdot\frac{y^{\langle m_i-k\rangle}}{(m_i-k)!}.$$

Hence we have

$$\det\left(\frac{(x^{l_j}y)^{\langle m_i\rangle}}{m_i!}\right)_{1\le i,j\le t} = \det\left(\begin{pmatrix} \frac{y^{\langle m_1\rangle}}{m_1!} & \frac{y^{\langle m_1-1\rangle}}{(m_1-1)!} & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ \frac{y^{\langle m_t\rangle}}{m_t!} & \frac{y^{\langle m_t-1\rangle}}{(m_t-1)!} & \cdots & \frac{y}{0!}\end{pmatrix}\begin{pmatrix} \frac{x^{l_1}}{0!} & \cdots & \frac{x^{l_t}}{0!}\\ \frac{(x^{l_1})^{\langle 1\rangle}}{1!} & \cdots & \frac{(x^{l_t})^{\langle 1\rangle}}{1!}\\ \vdots & \ddots & \vdots\\ \frac{(x^{l_1})^{\langle m_t\rangle}}{m_t!} & \cdots & \frac{(x^{l_t})^{\langle m_t\rangle}}{m_t!}\end{pmatrix}\right).$$

We denote by M and N the first and the second matrix of the right-hand side respectively. Then M is a $t \times (m_t + 1)$ matrix and N is an $(m_t + 1) \times t$ matrix. By the Binet-Cauchy formula,

$$\det(MN) = \sum_{1 \leq j_1 < \cdots < j_t \leq m_t + 1} |M|^{1 \ldots t}_{j_1 \ldots j_t} |N|^{j_1 \ldots j_t}_{1 \ldots t}.$$

It is easy to see that $|N|^{j_1 \ldots j_t}_{1 \ldots t} \in \mathbb{Z}[\lambda_i][x(v)]$. Therefore the proof of Claim 5 is reduced to proving the following:

Claim. Let $v \in \kappa^{-1}(\Theta^{[1]})$. Let $t \leq n$ be a positive integer. Let $0 \leq m_1 < \cdots < m_t \leq n - 1$ and $0 \leq k_1 < \cdots < k_t \leq m_t$. Then we have

$$(2y(v))^{n(n-1)/2} \det \left(\frac{y^{\langle m_i - k_j \rangle}(v)}{(m_i - k_j)!} \right)_{1 \leq i,j \leq t} \in \mathbb{Z}[\lambda_i][x(v), y(v)],$$

where we assume that $y^{\langle m \rangle}/m! = 0$ if $m < 0$.

For an integer $m \neq 0$, let $e(m) = 2m - 1$ and let $e(0) = 0$. By Lemma 5.6,

$$(2y(v))^{e(m)} \frac{y^{\langle m \rangle}(v)}{m!} \in \mathbb{Z}[\lambda_i][x(v), y(v)]$$

for any integer m. Since $e(m)$ is increasing with respect to m, if $m \leq m'$, then

$$(2y(v))^{e(m')} \frac{y^{\langle m \rangle}(v)}{m!} \in \mathbb{Z}[\lambda_i][x(v), y(v)].$$

By assumption, $m_i \leq n - 1 - t + i$ and $k_j \geq j - 1$. Hence we have $m_i - k_j \leq n - t + i - j$. Therefore, for any $1 \leq i, j \leq t$, there exists $b_{ij}(v) \in \mathbb{Z}[\lambda_i][x(v), y(v)]$ such that

$$\frac{y^{\langle m_i - k_j \rangle}(v)}{(m_i - k_j)!} = \frac{b_{ij}(v)}{(2y(v))^{e(n-t+i-j)}}.$$

Then we have

$$\begin{aligned} \det \left(\frac{y^{\langle m_i - k_j \rangle}(v)}{(m_i - k_j)!} \right)_{1 \leq i,j \leq t} &= \det \left(\frac{b_{ij}(v)}{(2y(v))^{e(n-t+i-j)}} \right)_{1 \leq i,j \leq t} \\ &= \sum_{\tau \in S_t} \operatorname{sgn}(\tau) \prod_{i=1}^{t} \frac{b_{i\tau(i)}(v)}{(2y(v))^{e(n-t+i-\tau(i))}}, \end{aligned}$$

where S_t is the symmetric group of degree t. Therefore it is sufficient to prove that

$$\sum_{i=1}^{t} e(n - t + i - \tau(i)) \leq \frac{n(n-1)}{2}$$

for any $\tau \in S_t$. The proof is divided into two cases.

Case 1. First we consider the case where $n-2t \geq 0$. Then $n-t+i-j \geq 1$ for all $1 \leq i, j \leq t$. Hence we have

$$\sum_{i=1}^{t} e(n-t+i-\tau(i)) = \sum_{i=1}^{t} (2(n-t+i-\tau(i))-1) = -2t^2+(2n-1)t.$$

Since n and t are integers, it is easily seen that $-2t^2+(2n-1)t \leq n(n-1)/2$.

Case 2. Next we consider the case where $n-2t < 0$. Let $l = n-2t$. Then $e(n-t+i-j) = 0$ if and only if $(i,j) \in \{(t-l+1,1),(t-l+2,2),\dots,(t,l)\}$. Note that $e(0) = 0 = (2\cdot 0-1)+1$. Hence we have

$$\sum_{i=1}^{t} e(n-t+i-\tau(i)) \leq l+\sum_{i=1}^{t} (2(n-t+i-\tau(i))-1) = -2t^2+(2n+1)t-n.$$

Since $n-2t$ is an integer and $n-2t<0$, we have $n-2t \leq -1$, that is, $t \geq (n+1)/2$. Therefore it is easily seen that $-2t^2+(2n+1)t-n \leq n(n-1)/2$. □

As an application of the determinantal expression, we can prove the following theorem:

Theorem 5.8. *There exists a non-zero element $\Delta \in \mathbb{Z}[\lambda_i]$ such that, for any integer n, $\phi_n \in \mathbb{Z}[1/\Delta, \lambda_i][\wp_{gi}, \wp_{ggi}]$.*

Proof. Without loss of generality, we may assume that $\lambda_0, \lambda_1, \dots, \lambda_{2g}$ are algebraically independent over $\mathbb{Q}$. By Proposition 4.3, we may assume that $n > 0$.

Let $E(u) = D(u^{(1)},\dots,u^{(g)})^2$. Since $D(u^{(1)},\dots,u^{(g)})$ is the Vandermonde determinant, $E(u)$ is a symmetric polynomial in $x(u^{(1)}),\dots,x(u^{(g)})$ with integral coefficients. Hence $E(u) \in \mathbb{Z}[\wp_{gi}]$ by Theorem 2.6.

For a non-negative integer m, let

$$Q_m(u) = \phi_n(u)E(u)^m.$$

Let M be the smallest integer such that $2M \geq n^2$. By Theorem 5.7,

$$Q_M(u) = F_n(u^{(1)},\dots,u^{(g)})D(u^{(1)},\dots,u^{(g)})^{2M-n^2}.$$

The right-hand side is symmetric with respect to $u^{(1)},\dots,u^{(g)}$. By using Theorem 2.6, we can eliminate $y(u^{(1)}),\dots,y(u^{(g)})$ in the right-hand side. Then the right-hand side becomes a symmetric polynomial in $x(u^{(1)}),\dots,x(u^{(g)})$ with coefficients in $\mathbb{Z}[1/2,\lambda_i][\wp_{ggi}]$. Therefore, by Theorem 2.6,

$$Q_M \in \mathbb{Z}[1/2,\lambda_i][\wp_{gi},\wp_{ggi}].$$

Then there exists a non-negative integer t such that

$$2^t Q_M \in \mathbb{Z}[\lambda_i][\wp_{gi},\wp_{ggi}].$$

For $m \geq 0$, let $Q'_m = 2^t Q_m$. Let $\Delta \in \mathbb{Z}[\lambda_i]$ be the element obtained by putting $S = E$ in Lemma 3.4. We prove that

$$Q'_m \in \mathbb{Z}[1/\Delta, \lambda_i][\wp_{gi}, \wp_{ggi}] \tag{16}$$

for $m \geq 0$ by induction on m.

When $m = M$, we have already proved (16). Assume that (16) holds for m. Since $Q'_m = Q'_{m-1}E$, (16) holds for $m-1$ by Lemma 3.4.

Since $\phi_n = Q'_0/2^t$, replacing Δ by 2Δ if necessary, the theorem holds. □

In Theorem 5.8, we only use $\wp_{g1}, \wp_{g2}, \ldots, \wp_{gg}, \wp_{gg1}, \wp_{gg2}, \ldots, \wp_{ggg}$ to express the division polynomial ϕ_n. If we use all the second and third derivatives, namely, $\wp_{11}, \wp_{12}, \ldots, \wp_{gg}$, $\wp_{111}, \wp_{112}, \ldots, \wp_{ggg}$, then we may be able to take a smaller element Δ. We illustrate this by the following example.

Example 5.9. We consider the case of genus 2.

First we use the defining equations F_1, F_2 in Example 2.10. By Theorem 2.6, we have

$$E(u) = D(u^{(1)}, u^{(2)})^2 = (x(u^{(2)}) - x(u^{(1)}))^2 = \wp_{22}(u)^2 + 4\wp_{12}(u).$$

Let $\tilde{S} = X_{22}^2 + 4X_{12}$ and G be a Gröbner basis for the ideal $\langle F_1, F_2, \tilde{S}\rangle$ in the ring $\mathbb{Z}[\lambda_i][X_{gi}, X_{ggi}]$. Then Theorem 5.8 holds for $\Delta = \Delta(G)$.

By computing the Gröbner basis G, we can compute Δ. The author used Macaulay 2 [13]. When we use degrevlex with $X_{122} > X_{222} > X_{12} > X_{22}$, we have $\Delta = 144 = 2^4 \cdot 3^2$. Therefore we have

$$\phi_n \in \mathbb{Z}[1/6, \lambda_i][\wp_{12}, \wp_{22}, \wp_{122}, \wp_{222}] \tag{17}$$

for any n.

We can also use all the second and third derivatives to represent ϕ_n. We use the defining equations F_3, F_4, F_5, F_6, F_7 in Example 2.11. We use degrevlex with

$$X_{111} > X_{112} > X_{122} > X_{222} > X_{11} > X_{12} > X_{22}.$$

Let G be a Gröbner basis for the ideal $\langle F_3, F_4, F_5, F_6, F_7, \tilde{S}\rangle$. Then we have $\Delta = \Delta(G) = 8 = 2^3$. Replacing Lemma 3.4 by Lemma 3.5 in the proof of Theorem 5.8, we have

$$\phi_n \in \mathbb{Z}[1/2, \lambda_i][\wp_{11}, \wp_{12}, \wp_{22}, \wp_{111}, \wp_{112}, \wp_{122}, \wp_{222}]$$

for any n. Moreover, by the defining equations F_3, F_4, F_6 in Example 2.11, we have the following relations:

$$\begin{aligned}
\wp_{112} &= \wp_{12}\wp_{222} - \wp_{122}\wp_{22},\\
\wp_{111} &= 2(\wp_{22} + \lambda_4)\wp_{112} - (\wp_{12} + \lambda_3)\wp_{122} - \wp_{11}\wp_{222},\\
4\wp_{11} &= -4(\wp_{22}^3 + \wp_{12}\wp_{22} + \lambda_4\wp_{22}^2 + \lambda_3\wp_{22} + \lambda_2) + \wp_{222}^2.
\end{aligned}$$

Therefore we have

$$\phi_n \in \mathbb{Z}[1/2, \lambda_i][\wp_{12}, \wp_{22}, \wp_{122}, \wp_{222}]$$

for any n, which is stronger than (17).

6. Recurrence formulas

In this section, we give recurrence formulas for the division polynomials. First, we review the following classical theta relation, which was independently proved by Caspary [10] and Frobenius [11].

Theorem 6.1. *Let $n > 2^g$ be an integer, $a, b \in (1/2)\mathbb{Z}^g$, $\tau \in \mathfrak{H}_g$ and $w_1, w_2, \ldots, w_n, z_1, z_2, \ldots, z_n \in \mathbb{C}^g$. Then we have*

$$\det\left(\vartheta\begin{bmatrix}a\\ b\end{bmatrix}(w_i+z_j,\tau)\,\vartheta\begin{bmatrix}a\\ b\end{bmatrix}(w_i-z_j,\tau)\right)_{1\le i,j\le n}=0.$$

Proof. See [10], [11] or [2, p. 473, Ex. v]. □

We obtain the following relation of the sigma functions as a corollary.

Corollary 6.2. *Let $n > 2^g$ be an integer and $u^{(1)}, u^{(2)}, \ldots, u^{(n)} \in \mathbb{C}^g$. We define the $n \times n$ matrix A by*

$$A=\left(\sigma(u^{(i)}+u^{(j)})\sigma(u^{(i)}-u^{(j)})\right)_{1\le i,j\le n}.$$

Then we have $\det A = 0$. In particular, if $g \equiv 1, 2 \pmod 4$ and n is even, then we have $\operatorname{pf} A = 0$.

Proof. The former part easily follows from Theorem 6.1 and the definition of the hyperelliptic sigma function. The latter part follows from Proposition 2.3. □

Remark 6.3. When $n = 2^g + 2$, the latter part of Corollary 6.2 was proved by Weierstrass [30].

By Corollary 6.2, we have the following relation of the division polynomials.

Theorem 6.4. *Let $n > 2^g$ be an integer, $m_1, m_2, \ldots, m_n$ be integers and $u \in \mathbb{C}^g$. We define the $n \times n$ matrix A by*

$$A=\left(\phi_{m_i+m_j}(u)\phi_{m_i-m_j}(u)\right)_{1\le i,j\le n}.$$

Then we have $\det A = 0$. In particular, if $g \equiv 1, 2 \pmod 4$ and n is even, then we have $\operatorname{pf} A = 0$.

Proof. By definition,

$$\phi_{m_i+m_j}(u)\phi_{m_i-m_j}(u)=\frac{\sigma(m_iu+m_ju)\sigma(m_iu-m_ju)}{\sigma(u)^{2(m_i^2+m_j^2)}}.$$

Hence we have

$$\begin{aligned}\det A &= \det\left(\frac{\sigma(m_iu+m_ju)\sigma(m_iu-m_ju)}{\sigma(u)^{2(m_i^2+m_j^2)}}\right)\\ &= \frac{1}{\sigma(u)^{4(m_1^2+\cdots+m_n^2)}}\det\bigl(\sigma(m_iu+m_ju)\sigma(m_iu-m_ju)\bigr)\\ &= 0\end{aligned}$$

by Corollary 6.2. The proof of the latter part is similar. □

We can derive recurrence formulas for the division polynomials from Theorem 6.4. We show examples for $g = 1, 2$.

Example 6.5. When $g = 1$ and $n = 4$, we have

$$\begin{aligned}&\phi_{m_1+m_2}(u)\phi_{m_1-m_2}(u)\phi_{m_3+m_4}(u)\phi_{m_3-m_4}(u)\\ &\quad-\phi_{m_1+m_3}(u)\phi_{m_1-m_3}(u)\phi_{m_2+m_4}(u)\phi_{m_2-m_4}(u)\\ &\quad+\phi_{m_1+m_4}(u)\phi_{m_1-m_4}(u)\phi_{m_2+m_3}(u)\phi_{m_2-m_3}(u)=0\end{aligned}$$

for any $m_1, \dots, m_4 \in \mathbb{Z}$. Putting $m_1 = k$, $m_2 = l$, $m_3 = m$ and $m_4 = 0$, we have

$$\begin{aligned}&\phi_{k+l}(u)\phi_{k-l}(u)\phi_m(u)^2-\phi_{k+m}(u)\phi_{k-m}(u)\phi_l(u)^2\\ &\qquad+\phi_{l+m}(u)\phi_{l-m}(u)\phi_k(u)^2=0.\end{aligned}$$

This is a well-known relation of the division polynomials in the case of genus 1 (cf. [27, Lemma 2.23]).

Example 6.6. Let $g = 2$ and $n = 6$. Putting $m_1 = m + 1$, $m_2 = m$, $m_3 = 3$, $m_4 = 2$, $m_5 = 1$ and $m_6 = 0$, we have

$$\begin{aligned}&\phi_{2m+1}(\phi_5-\phi_4\phi_2^3+\phi_3^3)\\ &\quad-\phi_{m+4}\phi_{m+2}\phi_{m-2}^2+\phi_{m+4}\phi_{m+1}\phi_{m-1}\phi_{m-2}\phi_2^2-\phi_{m+4}\phi_m^2\phi_{m-2}\phi_3\\ &\quad+\phi_{m+3}^2\phi_{m-1}\phi_{m-3}-\phi_{m+3}\phi_{m+1}\phi_{m-1}^2\phi_3^2+\phi_{m+3}\phi_m^2\phi_{m-1}\phi_4\phi_2\\ &\quad-\phi_{m+3}\phi_{m+2}\phi_m\phi_{m-3}\phi_2^2+\phi_{m+2}^2\phi_m\phi_{m-2}\phi_3^2-\phi_{m+2}\phi_m^3\phi_5\\ &\quad+\phi_{m+3}\phi_{m+1}^2\phi_{m-3}\phi_3-\phi_{m+2}\phi_{m+1}^2\phi_{m-2}\phi_4\phi_2+\phi_{m+1}^3\phi_{m-1}\phi_5=0,\end{aligned}\tag{18}$$

where we omit the variable u. Putting $m_1 = m + 1$, $m_2 = m - 1$, $m_3 = 3$, $m_4 = 2$, $m_5 = 1$ and $m_6 = 0$, we have

$$\begin{aligned}&\phi_{2m}\phi_2(\phi_5-\phi_4\phi_2^3+\phi_3^3)\\ &\quad-\phi_{m+4}\phi_{m+1}\phi_{m-2}\phi_{m-3}+\phi_{m+4}\phi_m\phi_{m-2}^2\phi_2^2-\phi_{m+4}\phi_{m-1}^2\phi_{m-2}\phi_3\\ &\quad+\phi_{m+3}\phi_{m+2}\phi_{m-1}\phi_{m-4}-\phi_{m+3}\phi_m\phi_{m-1}\phi_{m-2}\phi_3^2+\phi_{m+3}\phi_{m-1}^3\phi_4\phi_2\\ &\quad-\phi_{m+2}^2\phi_m\phi_{m-4}\phi_2^2+\phi_{m+2}\phi_{m+1}\phi_m\phi_{m-3}\phi_3^2-\phi_{m+2}\phi_m\phi_{m-1}^2\phi_5\\ &\quad+\phi_{m+2}\phi_{m+1}^2\phi_{m-4}\phi_3-\phi_{m+1}^3\phi_{m-3}\phi_4\phi_2+\phi_{m+1}^2\phi_m\phi_{m-2}\phi_5=0.\end{aligned}\tag{19}$$

To compute the division polynomials by the recurrence formulas (18) and (19), we need to prove that $\phi_5 - \phi_4\phi_2^3 + \phi_3^3 \neq 0$. We can verify it by direct computation or by using the Taylor expansion of the hyperelliptic sigma function.

In the case of genus 1, the recurrence formulas are used to compute the division polynomials. In the general case, the recurrence formulas are useful to compute the values of the division polynomials. Furthermore, at least theoretically, we can inductively compute the division polynomials by the recurrence formulas. However the computation requires division of hyperelliptic functions as described in Section 3, which is not efficient.

7. The canonical local height functions

In this section, we give explicit formulas for the canonical local height functions (or Néron functions) on the Jacobian J for Archimedean places. We also give a relation of the canonical local height function and the division polynomial.

First we review the canonical local height functions. For details, see [18, Chapter 11], [8], or [14, §B.9].

We assume that the hyperelliptic curve C is defined over a number field K. Then J and Θ are also defined over K. Let ϕ_n be the division polynomial of J defined as in Section 4. Then ϕ_n may be regarded as a rational function on J defined over K by Theorem 5.8. By definition, we have $[n]^*\Theta = n^2\Theta + \operatorname{div}(\phi_n)$ for $n \neq 0$.

Let M_K be the set of places of K. For each $v \in M_K$, let $|\cdot|_v$ be the absolute value associated with v whose restriction to $\mathbb{Q}$ is one of the standard absolute values on $\mathbb{Q}$. We define $v(x) = -\log|x|_v$. We denote the completion of K at v by K_v.

Definition 7.1. *A function $\lambda_v\colon (J \setminus \Theta)(K_v) \to \mathbb{R}$ is called a* local height function *for v (associated with Θ) if the following property holds: Let U be any Zariski open subset of J such that $U \cap \Theta \neq \emptyset$ and $\Theta|_U = \operatorname{div}(F)$ for some rational function F on U. Then there exists a continuous function $\alpha\colon U(K_v) \to \mathbb{R}$ such that*

$$\lambda_v(P) = v(F(P)) + \alpha(P)$$

for all $P \in (U \setminus \Theta)(K_v)$.

Definition 7.2. *Let $v \in M_K$. A function $\hat{\lambda}_v\colon (J\setminus\Theta)(K_v) \to \mathbb{R}$ is called the* canonical local height function *for v (associated with Θ) if the following conditions are satisfied.*

(i) *$\hat{\lambda}_v$ is a local height function for v associated with Θ.*
(ii) *Let ϕ be a rational function on J satisfying $[2]^*\Theta = 4\Theta + \operatorname{div}(\phi)$. Then*

$$\hat{\lambda}_v([2]P) = 4\hat{\lambda}_v(P) + v(\phi(P))$$

for all $P \in (J \setminus \Theta)(K_v)$.

The canonical height function $\hat{\lambda}_v$ is uniquely determined up to an additive constant. Furthermore, if we fix the function ϕ, then $\hat{\lambda}_v$ is uniquely determined.

The division polynomial ϕ_2 satisfies $[2]^*\Theta = 4\Theta + \operatorname{div}(\phi_2)$. From now on, we fix $\phi = \phi_2$. Then $\hat{\lambda}_v$ is uniquely determined.

To describe an explicit formula for the canonical local height function for an Archimedean place, we make some definitions. Let v be an Archimedean place. Then there exists an embedding $\tau\colon K_v \hookrightarrow \mathbb{C}$ corresponding to v such that $|x|_v = |\tau(x)|$ for all $x \in K_v$, where the absolute value in the right-hand side is the usual one. We identify K_v as a subfield of $\mathbb{C}$ through the embedding τ.

We define the function $\Sigma(u)$ on $\mathbb{C}^g$ by

$$\Sigma(u) = \boldsymbol{e}\left(-\frac{1}{2}L(u,u)\right)\sigma(u).$$

Proposition 7.3. *The function $|\Sigma(u)|$ on $\mathbb{C}^g$ is periodic with respect to Λ.*

Proof. Let $l \in \Lambda$. By Proposition 2.2, we have

$$|\Sigma(u+l)| = \left|\boldsymbol{e}\left(\frac{1}{2}E(u,l)\right)\right| \cdot |\Sigma(u)|.$$

By Proposition 2.4 (i), $E(u,l) \in \mathbb{R}$. Therefore we have

$$\left|\boldsymbol{e}\left(\frac{1}{2}E(u,l)\right)\right| = 1.$$

This proves the proposition. □

Then we have the following explicit formula:

Theorem 7.4. *Let $P \in (J \setminus \Theta)(K_v)$. Let $u \in \mathbb{C}^g$ be a point with $\kappa(u) = P$. Then we have*

$$\hat{\lambda}_v(P) = v(\Sigma(u)).$$

Proof. We define the function $\hat{\lambda}'_v \colon (J \setminus \Theta)(K_v) \to \mathbb{R}$ by

$$\hat{\lambda}'_v(P) = v(\Sigma(u)),$$

where $u \in \mathbb{C}^g$ satisfies $\kappa(u) = P$. By Proposition 7.3, $\hat{\lambda}'_v$ is well-defined. It is sufficient to prove that the conditions in Definition 7.2 are satisfied. Then the theorem follows from the uniqueness of the canonical local height function.

First we prove that $\hat{\lambda}'_v$ is a local height function associated with Θ. Let U be a Zariski open subset of J such that $U \cap \Theta \neq \emptyset$ and $\Theta|_U = \operatorname{div}(F)$ for some rational function F on U. Let $G(u) = \sigma(u)/F(\kappa(u))$. Since $\operatorname{div}(G) = 0$, G and $1/G$ are holomorphic functions on $\kappa^{-1}(U)$. Therefore $v(G(u))$ is continuous on $\kappa^{-1}(U)$. By the definition of $\hat{\lambda}'_v$, we have

$$\hat{\lambda}'_v(P) = v(F(P)) + v(G(u)) - \pi \operatorname{Im} L(u,u),$$

where $P = \kappa(u)$. Therefore $\hat{\lambda}'_v$ is a local height function associated with Θ.

Next we prove that

$$\hat{\lambda}'_v([2]P) = 4\hat{\lambda}'_v(P) + v(\phi_2(P)).$$

By definition,

$$\begin{aligned}
\hat{\lambda}'_v([2]P) &= v\left(\boldsymbol{e}\left(-\frac{1}{2}L(2u,2u)\right)\sigma(2u)\right) \\
&= 4v\left(\boldsymbol{e}\left(-\frac{1}{2}L(u,u)\right)\sigma(u)\right) + v\left(\frac{\sigma(2u)}{\sigma(u)^4}\right) \\
&= 4\hat{\lambda}'_v(P) + v(\phi_2(P)).
\end{aligned}$$

This concludes the proof of the theorem. □

From now on, we consider an arbitrary place. We have translation formulas for the canonical local height functions as follows:

Theorem 7.5. *Let $v \in M_K$ and $P, Q \in (J \setminus \Theta)(K_v)$.*

(i) *(Quasi-parallelogram low) If $P+Q, P-Q \notin \Theta$, then we have*

$$\hat{\lambda}_v(P+Q) + \hat{\lambda}_v(P-Q) = 2\hat{\lambda}_v(P) + 2\hat{\lambda}_v(Q) + v(\mathcal{F}_g(P,Q)).$$

(ii) *Let n be a non-zero integer. If $[n]P \notin \Theta$, then we have*

$$\hat{\lambda}_v([n]P) = n^2\hat{\lambda}_v(P) + v(\phi_n(P)).$$

Note that Theorem 7.5 immediately follows from Theorem 7.4 when v is Archimedean. In the following, we prove Theorem 7.5 for an arbitrary place.

Proof. First note that it is sufficient to prove the corollary on $U(K_v)$, where U is a non-empty Zariski open subset of J, since the functions appearing in the proof are v-adically continuous. Hence we will not specify the domains of the functions.

(i) Let $\sigma, \delta, \pi_1, \pi_2 \colon J \times J \to J$ be the homomorphisms defined by

$$\sigma(P,Q) = P+Q, \quad \delta(P,Q) = P-Q, \quad \pi_1(P,Q) = P, \quad \pi_2(P,Q) = Q.$$

Then we have

$$\operatorname{div} \mathcal{F}_g = \sigma^*\Theta + \delta^*\Theta - 2\pi_1^*\Theta - 2\pi_2^*\Theta.$$

Therefore, by general theory (cf. [18, §11, Theorem 1.1]), there exists a constant γ_v such that

$$\hat{\lambda}_v(P+Q) + \hat{\lambda}_v(P-Q) = 2\hat{\lambda}_v(P) + 2\hat{\lambda}_v(Q) + v(\mathcal{F}_g(P,Q)) + \gamma_v. \tag{20}$$

Substituting $[2]P$ and $[2]Q$ for P and Q respectively, we have

$$\begin{aligned}\hat{\lambda}_v([2](P+Q)) + \hat{\lambda}_v([2](P-Q)) \\ = 2\hat{\lambda}_v([2]P) + 2\hat{\lambda}_v([2]Q) + v(\mathcal{F}_g([2]P,[2]Q)) + \gamma_v.\end{aligned} \tag{21}$$

On the other hand, by Proposition 4.9,

$$\begin{aligned}v(\phi_2(P+Q)) + v(\phi_2(P-Q)) \\ = 2v(\phi_2(P)) + 2v(\phi_2(Q)) - 4v(\mathcal{F}_g(P,Q)) + v(\mathcal{F}_g([2]P,[2]Q)).\end{aligned} \tag{22}$$

Combining (20), (21), (22), and the definition of $\hat{\lambda}_v$, we have $\gamma_v = 0$.

(ii) We prove it by induction on n. If $n = 1, 2$, it is clear by definition.

Let $n \geq 3$. We assume that the corollary holds for $n-1$ and $n-2$. Then, by (i),

$$\begin{aligned}\hat{\lambda}_v([n]P) &= -\hat{\lambda}_v([n-2]P) + 2\hat{\lambda}_v([n-1]P) + 2\hat{\lambda}_v(P) + v(\mathcal{F}_g([n-1]P,P)) \\ &= -(n-2)^2\hat{\lambda}_v(P) - v(\phi_{n-2}(P)) + 2(n-1)^2\hat{\lambda}_v(P) \\ &\quad + 2v(\phi_{n-1}(P)) + 2\hat{\lambda}_v(P) + v(\mathcal{F}_g([n-1]P,P)) \\ &= n^2\hat{\lambda}_v(P) + v(\phi_n(P)).\end{aligned}$$

This completes the proof. □

Remark 7.6. Theorems 7.4 and 7.5 are already known in the case of genus 1 (cf. [28, Chapter VI]). Note that our canonical local height function differs from that in [28] by an additive constant.

In the case of genus 2, Theorem 7.4 was proved by Yoshitomi [32, Corollary 2.5]. The author has proved formulas similar to Theorem 7.5. The details will appear in a forthcoming publication.

Acknowledgements. The author would like to thank Professors Kenichi Bannai, Kazuhiro Fujiwara, Atsushi Moriwaki, and Yoshihiro Ônishi for valuable comments and help. He also would like to thank the referee for useful comments and suggestions. He was partially supported by the JSPS Research Fellowships for Young Scientists and the JSPS Core-to-Core Program 18005.

References

[1] Adams, W. W., Loustaunau, P.: An Introduction to Gröbner bases. Graduate Studies in Mathematics 3, American Mathematical Society, Providence (1994)
[2] Baker, H. F.: Abelian Functions: Abel's theorem and the allied theory of theta functions. Cambridge University Press, Cambridge (1897)
[3] Baker, H. F.: On a system of differential equations leading to periodic functions. Acta Math. **27**, 135–156 (1903)
[4] Baker, H. F.: An Introduction to the Theory of Multiply Periodic Functions. Cambridge University Press, Cambridge (1907)
[5] Buchstaber, V. M., Enolskii, V. Z., Leykin, D. V.: Kleinian functions, hyperelliptic Jacobians and applications. Rev. Math. Math. Phys. **10**, 1–125 (1997)
[6] Buchstaber, V. M., Enolskii, V. Z., Leykin, D. V.: A recursive family of differential polynomials generated by the Sylvester identity and addition theorems for hyperelliptic Kleinian functions. Funct. Anal. Appl. **31**, 240–251 (1997)
[7] Bukhshtaber, V. M., Leikin, D. V., Enol'skii, V. Z.: σ-functions of (n, s)-curves. Russ. Math. Surv. **54**, 628–629 (1999)
[8] Call, G. S., Silverman, J. H.: Canonical heights on varieties with morphisms. Compos. Math. **89**, 163–205 (1993)
[9] Cantor, D. G.: On the analogue of the division polynomials for hyperelliptic curves. J. reine angew. Math. **447**, 91–145 (1994)
[10] Caspary, F.: Zur Theorie der Thetafunctionen mehrerer Argumente. J. reine angew. Math. **96**, 324–326 (1884)
[11] Frobenius, G.: Ueber Thetafunctionen mehrerer Variabeln. J. reine angew. Math. **96**, 100–122 (1884)
[12] Grant, D.: Formal groups in genus two. J. reine angew. Math. **411**, 96–121 (1990)
[13] Grayson, D. R., Stillman, M. E.: Macaulay 2, a software system for research in algebraic geometry. `http://www.math.uiuc.edu/Macaulay2/`
[14] Hindry, M., Silverman, J. H.: Diophantine Geometry: An Introduction. Graduate Texts in Mathematics 201, Springer-Verlag, New York (2000)
[15] Kanayama, N.: Division polynomials and multiplication formulae of Jacobian varieties of dimension 2. Math. Proc. Camb. Philos. Soc. **139**, 399–409 (2005)
[16] Kanayama, N.: Corrections to "Division polynomials and multiplication formulae in dimension 2." Math. Proc. Camb. Philos. Soc. **149**, 189–192 (2010)
[17] Lang, S.: Introduction to Algebraic and Abelian Functions. Second edition, Graduate Texts in Mathematics 89, Springer-Verlag, New York (1982)

[18] Lang, S.: Fundamentals of Diophantine Geometry. Springer-Verlag, New York (1983)
[19] Maxima.sourceforge.net, Maxima, a Computer Algebra System. Version 5.18.1, http://maxima.sourceforge.net/ (2009)
[20] Mumford, D.: Tata Lectures on Theta I. Progress in Mathematics 28, Birkhäuser, Boston (1983)
[21] Mumford, D.: Tata Lectures on Theta II. Progress in Mathematics 43, Birkhäuser, Boston (1984)
[22] Nakayashiki, A.: On algebraic expressions of sigma functions for (n, s) curves. arXiv:0803.2083v1 [math.AG]
[23] Noro, M. et al.: A computer algebra system Risa/Asir. http://www.math.kobe-u.ac.jp/Asir/
[24] Ônishi, Y.: Determinant expressions for Abelian functions in genus two. Glasg. Math. J. **44**, 353–364 (2002)
[25] Ônishi, Y.: Determinantal expressions for hyperelliptic functions in genus three. Tokyo J. Math. **27**, 299–312 (2004)
[26] Ônishi, Y.: Determinant expressions for hyperelliptic functions (with an appendix by Shigeki Matsutani). Proc. Edinb. Math. Soc. **48**, 705–742 (2005)
[27] Schmitt, S., Zimmer, H. G.: Elliptic Curves: A Computational Approach. de Gruyter Studies in Mathematics 31, Walter de Gruyter, Berlin (2003)
[28] Silverman, J. H.: Advanced Topics in the Arithmetic of Elliptic Curves. Graduate Texts in Mathematics 151, Springer-Verlag, New York (1994)
[29] van der Waerden, B. L.: Algebra. Volume 2, Ungar, New York (1970)
[30] Weierstrass, K.: Zur Theorie der Jacobi'schen Functionen von mehreren Veränderlichen. Sitzung. Königlich Preuss. Akad. Wiss. Berl. 505–508 (1882); Mathematische Werke III, Johnson Reprint Corporation, New York, 155–159 (1967)
[31] Whittaker, E. T., Watson, G. N.: A Course of Modern Analysis. Fourth edition, Cambridge University Press, Cambridge (1927)
[32] Yoshitomi, K.: On height functions on Jacobian surfaces. Manuscr. math. **96**, 37–66 (1998)